The High Level Panel of Legal Experts on Media Freedom

The independent advisory body to the Media Freedom Coalition

International Bar Association
Human Rights Institute

Speech related to National Security: Espionage and Official Secrets Laws

Authors: Ms Amal Clooney and Ms Alice Gardoll

Excerpt from *Freedom of Speech in International Law* (edited by Lord David Neuberger and Ms Amal Clooney, published by Oxford University Press).


INTERNATIONAL BAR ASSOCIATION
Human Rights Institute

This IBAHRI publication is an extracted chapter of Freedom of Speech in International Law, edited by Lord David Neuberger of Abbotsbury and Ms Amal Clooney and published by Oxford University Press in January 2024. The authors of this chapter are Ms Amal Clooney and Ms Alice Gardoll. Ms Alice Gardoll is the Assistant Editor of the text. The full text can be purchased in hard copy or as an e-book **here**. All sources and references have been checked for accuracy as of 1 January 2022.

Freedom of Speech in International Law outlines the minimum protections for speech enshrined in international law, focusing on four types of laws that are being weaponized to silence the press and independent voices: laws regulating defamatory or insulting speech, laws regulating false speech, laws regulating hate speech and laws regulating national security. The book provides examples of where states are falling short and makes recommendations about how international standards should be interpreted, updated and enforced.

Recommendations are based on international legal standards that apply to states and that many social media companies have expressed adherence to. The recommendations have been endorsed by the High Level Panel of Legal Experts on Media Freedom, as well as judges and experts from across the world including the Committee to Protect Journalists, Reporters without Borders, the UN Special Rapporteur on Freedom of Expression and the International Bar Association's Human Rights Institute.

The International Bar Association's Human Rights Institute, serves as Secretariat to the High Level Panel of Legal Experts on Media Freedom, providing it with operational, technical, and legal assistance. The work of the High Level Panel, including the research contained in this report, has been supported by the Global Media Defence Fund, administered by UNESCO. At the time of publication, the Chair of the High Level Panel was Lord Neuberger of Abbotsbury and its Deputy Chairs were Professor Can Yeginsu and Ms. Catherine Amirfar.

Cover image: **www.stock.adobe.com**

www.ibanet.org/IBAHRI

5

Speech Related to National Security: Espionage and Official Secrets Laws

Amal Clooney and Alice Gardoll

I. Introduction 4
II. State Practice 7
1. Overview of Laws Regulating Disclosure of 'Secret' Material 7
1.1. Type of speech 7
1.2. Harm 10
1.3. Intent 11
1.4. Exclusions, exceptions and defences 12
1.5. Penalties 14
2. Application of Espionage and Official Secrets Laws Around the World 15
2.1. Europe and United Kingdom 15
2.2. Asia Pacific 20
2.3. Middle East and Africa 25
2.4. North and South America 27
III. International Legal Standards 33
1. International Standards Related to Speech Affecting National Security 34
2. Legality 40
3. Legitimacy 42
4. Necessity 43
4.1. Secrecy 45
4.2. Harm 47
4.3. Intent 52
5. Exclusions, Exceptions and Defences 52
5.1. Public interest defence 52
5.2. Reasonableness of the publication 56
5.3. Truth 60
5.4. Opinion 61
6. Penalties 61
IV. Recommendations 64

I. Introduction

The principle that certain speech can be penalized if it jeopardizes national security, defence, military operations or diplomatic relations is not controversial.[1] Laws providing for the secrecy of some government information are ubiquitous across democracies and authoritarian regimes alike. But legal responses to the disclosure of material deemed secret by the state vary widely. Some states classify limited information as secret and accept a culture of leaking, either through prosecutorial discretion or laws that allow such conduct. Others, including democratic states, clamp down heavily on the disclosure of any government-derived information whether it is classified or not.

A striking feature of this area of the law is that leading democracies that are generally considered protective of speech are among the governments with particularly

[1] The authors and editors are grateful for the excellent research and work done by Professor Vincent Wong of the University of Windsor Faculty of Law and his clinical students in relation to this chapter. Professor Wong served as the lead project manager at the University of Toronto Law School on the media freedom initiative led by the High-Level Panel of Legal Experts on Media Freedom, an expert group established at the behest of the governments of Canada and the United Kingdom.

harsh laws and practices. One example is the United Kingdom. The UK Official Secrets Act, originally enacted in 1889, has been widely criticized as one of the most illiberal iterations of official secrets laws.[2] Prior to its 1989 amendments, any unauthorized disclosure of official information entrusted to a Crown servant by a state official was prohibited, regardless of the level of secrecy of a document, the harm it may have caused or the individual's intention.[3] And although this law has only been used in a small number of high-profile cases in the United Kingdom,[4] due to Britain's colonial reach, iterations of this law were adopted in British colonies across the globe. Many former colonies maintain these laws, with the result that legislation that significantly curtails speech related to 'secret' material applies to millions of people across the world from Uganda and Zimbabwe to India, Pakistan, Sri Lanka, Myanmar, Singapore and Malaysia.[5]

Similarly, the United States, one of the most speech-friendly states in the world thanks to its First Amendment jurisprudence,[6] has in recent years made significant recourse to espionage laws to clamp down on speech. Prior to 2009, only a handful of prosecutions for disclosing confidential information to the press had ever taken place under the US Espionage Act, even though the United States has a 'longstanding culture of leaking', with press breaking a number of high-profile stories on the basis of leaks.[7] This included revealing the CIA's use of secret prisons and the human rights abuses at the Abu Ghraib detention facility in Iraq.[8] But both the Obama and Trump administrations increased prosecutions of government sources under the Espionage Act in an unprecedented manner. And the indictment of Wikileaks' Julian Assange represents the first time an individual who *published* classified information has been successfully indicted, raising the spectre that traditional journalists are no longer off limits for prosecution under a law intended to catch spies.[9] Recent US prosecutorial practice has therefore applied the US

[2] See, e.g., C. W. Cheong, 'Section 5 of the Official Secrets Act, Bridges and Beyond' (1998) 2 *Singapore Journal of Legal Studies* 260, 261. Unless otherwise indicated, references to the United Kingdom and the UK refer to England and Wales, Scotland, and Northern Ireland. Although many of the same laws apply across these jurisdictions, these laws can vary and Scotland has a separate legal system.

[3] See UK Official Secrets Act, s. 2. See UK Law Commission, *Protection of Official Data Report* (2020), §§4.4–4.6; G. Bartlett & M. Everett, 'Briefing Paper: The Official Secrets Act and Official Secrecy' (House of Commons Library, 2 May 2017), 18–21.

[4] Bartlett & Everett (n 3) (listing 12 '[n]otable cases involving the Official Secrets Act or leaks of Government information'). See s. II.2.1.1. (United Kingdom).

[5] Indian Official Secrets Act 1923; Pakistani Official Secrets Act 1923; Malaysian Official Secrets Act 1972; Myanmar Official Secrets Act 1923; Singaporean Official Secrets Act 1935; Sri Lankan Official Secrets Act, No. 32 of 1955; Ugandan Official Secrets Act 1964, ch. 302; Zimbabwean Official Secrets Act 1970.

[6] A number of sources chart the US Supreme Court's historical path towards this more speech protective position: see, e.g., M. Rosenfeld, 'Hate Speech in Constitutional Jurisprudence: A Comparative Analysis', in M. Herz & P. Molnar (eds), *The Content and Context of Hate Speech: Rethinking Regulation and Responses* (CUP 2012); E. Bleich, 'Freedom of Expression versus Racist Hate Speech: Explaining Differences Between High Court Regulation in the USA and Europe' (2013) 40(2) *Journal of Ethnic and Migration Studies* 283. See ch. 1 (Introduction), ss II.1.2.1.2. (ICCPR: Article 20) and II.1.2.1.3. (CERD: Article 4) discussing US reservations.

[7] See, e.g., Knight First Amendment Institute at Columbia University, 'Press-related prosecutions under the Espionage Act'; K. Feuer, 'Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act' (2015) 38(1) *Boston College International and Comparative Law Review* 91, 95.

[8] Ibid., 98.

[9] See s. II.2.4.3. (United States: Julian Assange). See also G. Rottman, 'Special Analysis of the May 2019 Superseding Indictment of Julian Assange' (Reporters Committee, 30 May 2019).

Espionage Act in a way that creates a glaring exception to the United States' proud history of free speech protection and 'potentially opens the door for journalists anywhere in the world to be extradited to the US for exposing information deemed classified by Washington'.[10]

A central tension within this area of the law is the relevance of the 'public interest' in assessing whether speech should be unlawful. International standards dictate, at a minimum, that both the public interest in the speech and the potential harm to national security arising from speech are relevant to determining whether it is legally 'necessary' to penalize it using civil or criminal sanctions.[11] However, many national laws do not reflect this standard, either on paper or in practice, and many autocratic governments brand journalists as 'spies' and use 'national security' as a pretext to stifle the press as well as ordinary citizens.[12]

This disconnect has led to increasing calls for reform. The Global Principles on National Security and the Right to Information (known as the Tshwane Principles), drafted in 2013 in consultation with over 500 legal experts, including civil society actors and government officials, support an affirmative public interest defence, and have been endorsed by five UN and regional Special Rapporteurs and the Parliamentary Assembly for the Council of Europe.[13] The Law Commission of England and Wales also recently recommended an amendment of the UK Official Secrets Act to allow a public interest defence to prosecutions of speech that reveals government secrets.[14]

This chapter considers state practice in this area,[15] international standards governing the language and use of such laws[16] and recommendations as to how such laws should be drafted, interpreted and applied to comply with international law and best practices.[17]

[10] 'The Guardian view on Julian Assange's extradition: a bad day for journalism' (The Guardian, 17 June 2022).

[11] See s. II.1.2. (Harm) and s. III.5.1. (Public interest defence).

[12] See, e.g., CPJ, 'Database of attacks on the press—Journalists imprisoned between 1992 and 2020' (concerning data on journalists imprioned between 1992 and 2020 for 'anti-state' charges). See also ss II.2.1.2. (Slovenia); II.2.2.2. (Australia); II.2.2.3. (Cambodia).

[13] Tshwane Principles. See s. III.1. (International Standards Related to Speech Affecting National Security).

[14] See UK Law Commission, *Protection of Official Data Report* (2020).

[15] The definition of 'official secret' or 'espionage' varies by jurisdiction, and neither has a consistent interpretation under international law. For the purposes of this chapter, 'official secrets' or 'state secrets' refer to confidential or classified information held by a public authority, and protected against unauthorized disclosure on grounds such as national security and intelligence, or international relations. 'Espionage' is understood as referring to unlawfully obtaining information held in confidence by the government, usually (but not always) for the benefit of another state or foreign power. Although espionage laws generally encompass a range of offences related to 'spying' that extend beyond speech-related conduct, such as theft, this chapter focuses on espionage laws which capture 'pure speech' behaviour, and takes no position on the need or appropriateness of more traditional 'spying' provisions under international law.

[16] This chapter does not examine the corollary right to *receive* information that is relevant to official secrets laws. Protection of sources and materials, as well as whistle-blowing regimes that protect public officials or contractors from civil and administrative repercussions are also not within the scope of this chapter.

[17] See s. IV. (Recommendations).

II. State Practice

1. Overview of Laws Regulating Disclosure of 'Secret' Material

Laws regulating disclosure of 'secret' material—usually espionage or 'official secrets' legislation—exist in states across the globe.[18] All of the laws surveyed in this chapter include criminal penalties for unauthorized disclosures.[19]

But the requirements for penalization set out in these laws—including the scope of the speech that is covered, the required intent of the speaker, harm caused by the speech, defences and penalties—differ considerably. Some states prohibit the disclosure of *any* governmental information while others require that information to be 'secret' or 'classified', and also define these terms differently. States define harm differently and a large number of states do not set out any harm requirement at all, perhaps on the assumption that some harm always results from the disclosure of 'secret' information. Penalties also significantly vary, although many states' laws provide for heavy maximum penalties of between 10–15 years' imprisonment for spilling secrets through speech. Only a small number of countries have an affirmative public interest defence, and even those that do can be narrowly worded. These include Canada, Australia, Denmark and Slovenia, while countries such as the United Kingdom and the United States are yet to adopt such a defence despite strong calls for them to do so.[20]

In certain nations, special approvals are needed before a prosecution under espionage or official secrets laws can be triggered. This is the case, for instance, in the United Kingdom, Ghana, Singapore and Australia, although a number of earlier steps such as arrest and charges can take place in Australia without such consent.[21] And prosecutorial guidance in Canada and the United States establishes approval procedures for certain prosecutions, including official secrets charges.[22]

1.1. Type of speech

Many state laws use vague wording or fail to define key terms in official secrets laws such as 'secret', 'confidential' or 'national security'. Examples include Cambodia, where 'facilitating easy access' by foreign agents to information which 'undermines the national security' is criminalized with up to 15 years' imprisonment, and Myanmar, which criminalizes obtaining, collecting, recording, publishing or communicating

[18] The review of state official secrets and espionage laws and practice contained in this chapter does not aim to be comprehensive but rather to identify significant examples and trends. In addition, references to the language of a statute are not necessarily accompanied by an analysis of all case law interpreting that language in the jurisdiction under review.

[19] This chapter reviews 46 countries' laws related to espionage and official secrets.

[20] See s. II.1.4.1. (Public interest).

[21] See UK Official Secrets Act 1989 s. 9 (requiring consent for the prosecution of offences based on unauthorized disclosure of official information); Australian Criminal Code s. 93.1; Singaporean Official Secrets Act s. 14; Ghanian State Secrets Act 1962 (Act 101) s. 11.

[22] Public Prosecution Service of Canada, *Public Prosecution Service of Canada Deskbook, Guideline of the Director Issued under Section 3(3)(c) of the Director of Public Prosecutions Act* (2021); US Department of Justice, *Justice Manual: Title 9-90.020, National Security Matters.*

information which might be 'directly or indirectly, useful to an enemy' if this is done 'for any purpose prejudicial to the safety and interests' of the state.[23] A number of laws have not been amended since their enactment many decades ago and use language such as 'enemy' which may be poorly suited to modern day national security concerns.[24]

1.1.1. Secrecy

The 'secrecy' element of official secrets laws has several components: whether governmental information must be classified as 'secret' to be unlawfully disclosed, how secrecy is defined, and whether all persons are captured by the law or only those who owe a duty of secrecy.

Certain official secrets and espionage laws prohibit the possession or communication of certain governmental information with no additional 'secrecy' requirement. For example, the US Espionage Act applies to 'information respecting the national defense'.[25] US courts have interpreted this section as not requiring that information is classified, although the government must, as a preliminary matter, show that steps were taken to maintain its secrecy. Similarly, US courts have found that the classification of a document alone may be sufficient to prove its link to national defence.[26]

A number of countries prohibit the disclosure of any 'secret' or 'secret official' information, consistent with early versions of the UK Official Secrets Act that were imported into Commonwealth countries' laws across the world.[27] For example, Singapore's Official Secrets Ordinance provides criminal penalties for communicating directly or indirectly 'any secret official code word, countersign or password, or any photograph, drawing, plan, model, article, note, document or information' obtained in contravention of the Act.[28] But Singaporean courts have interpreted this provision as capturing two types of expression: any 'word, countersign or password', which must be 'secret official', and the other listed types of expression, which do not have to be 'secret official'.[29]

Similarly the United Kingdom's official secrets laws criminalize the disclosure of six categories of information: information relating to 'security and intelligence';[30] 'defence';[31] 'international relations';[32] information the disclosure of which 'results in the commission of an offence' or impacts law enforcement efforts;[33] information acquired

[23] Cambodian Criminal Code 2009 Art. 445; Myanmar Official Secrets Act s. 3(1)(c).

[24] See, e.g., 18 U.S.C. § 794(b) (this chapter uses the shorthand term the US Espionage Act to describe the current provisions in the Unites States Code that were originally enacted as the US Espionage Act).

[25] Ibid., s. 793.

[26] Feuer (n 7) 91, 117, citing US District Court, District of Columbia, *United States v. Kim* 808 F. Supp. 2d 44, 24 August 2011, 55 and US Court of Appeals, Fourth Circuit, *United States v. Morison* 844 F.2d 1057, 1 April 1988, 1074.

[27] See Bangladeshi Official Secrets Act 1923 s. 5(1) (except to a person to whom one is 'authorized to communicate' the information, or to a 'Court of Justice or a person to whom it is, in the interests of the State, one's duty to communicate' the information); Ugandan Official Secrets Act 1964 ch. 302 s. 4.

[28] Singaporean Official Secrets Act s. 5(1).

[29] Cheong (n 2), 263–264, citing Singapore High Court, *Public Prosecutor v Bridges Christopher* [1998] 3 SLR 467 (CA).

[30] UK Official Secrets Act 1989 s. 1(1).

[31] Ibid., s. 2.

[32] Ibid., s. 3.

[33] Ibid., s. 4.

by a civil servant;[34] and information related to security, intelligence, defence or international relations 'communicated in confidence by or on behalf of the United Kingdom to another State or to an international organisation'.[35] These categories, with the exception of the final one, do not require information to be secret or classified.

Other states have more precise definitions of secrecy. For instance, Germany defines state secrets as 'facts, objects or knowledge' accessible to a limited category of persons and which must be kept secret 'from foreign powers in order to avert a danger of serious prejudice to the external security' of Germany.[36] Other nations, such as Slovenia, Peru and El Salvador link secrecy to the classification of information by certain government bodies.[37]

1.1.2. Who does the duty of secrecy apply to?

Although many espionage and official secrets laws apply to all persons,[38] some states have legislation that limits penalties for publishing state secrets to government officials, employees or those with a specific duty of secrecy. For example, in Georgia a person can only be responsible for the disclosure of a secret if they had an official duty or civil agreement to protect its confidentiality and the disclosure 'creates obvious, direct and essential danger, to the interests protected under the law'.[39] Some countries limit criminal responsibility for disclosure of official secrets to public officials.[40] Germany's criminal law was amended in 2012 to ensure that journalists cannot be charged with aiding the 'violation of official secrets' for disclosing classified information.[41] And a number of states provide lesser penalties for unauthorized disclosures of secret information by private persons rather than public officials.[42]

1.1.3. Type of disclosure

Laws vary as to what conduct relating to official secrets is prohibited. States such as Albania do not punish the possession of secret information, only its disclosure or use.[43] But states such as the United States and Canada prohibit mere receipt and retention of secret information.[44] Similarly, a number of countries whose laws are modelled on early versions of the UK Official Secrets Act continue to penalize a wide range of acts,

[34] Ibid., s. 5.
[35] Ibid., s. 6.
[36] German Criminal Code s. 93.
[37] Slovenian Criminal Code Art. 260(1); Peruvian Legislative Decree 1141 Art. 4; El Salvador State Intelligence Body Law Decree No. 554 Art. 8.
[38] See, e.g., 18 U.S.C. §793; UK Official Secrets Act 1989 ss 5–6; Canadian Security of Information Act s. 4; Indonesian Law No. 17 of 2011 Art. 26; Japan's Act on the Protection of Specially Designated Secrets No. 108 of 2013 Art. 24.
[39] Georgian Law on Freedom of Speech and Expression, as amended in 2012, Art. 12.
[40] See, e.g., Moldovan Criminal Code Art. 344 (although this provision also covers individuals who are not necessarily public officials but to whom information 'was entrusted' or 'became known in connection with his/her official position or professional duties'); Colombian Criminal Code Art. 418.
[41] German Criminal Code s. 353(b)(3a).
[42] See, e.g., Belgian Penal Code Art. 118; Bolivian Penal Code Art. 116; German Criminal Code ss 94–96; Panamanian Criminal Code Art. 428; Ugandan Official Secrets Act of 1964 ch. 302 s. 15; Ugandan Security Organisations Act (1987) ch. 305 s. 10.
[43] Albanian Criminal Code Arts 213, 214, 294, 295. Cf. Albanian Criminal Code Art. 296 (criminalizing 'loss' of secret documents).
[44] 18 U.S.C. §793(e). See s. II.2.4.3. (United States: Julian Assange); Canadian Security of Information Act s. 4.

such as retaining information 'when he has no right to retain it'.[45] Australia's espionage and state secrets laws capture any manner of 'dealing' with such information, which encompasses receiving, collecting, reviewing, possessing, making a record of, copying, altering, concealing or making available information in addition to disclosing it.[46] And some nations criminalize both disclosure and lesser forms of conduct such as possession but provide differing criminal penalties depending on the conduct in question.[47]

1.2. Harm

Official secrets laws are grounded in the idea that speech disclosing confidential official material harms the government. And yet the requirement that the disclosure in question in fact does cause harm, or is reasonably likely to do so, is not always present in official secrets laws. And in the case of laws that do incorporate such a requirement, the definition of damage or harm can be expansive, or presumed to be met without proof if certain conditions are satisfied.

Nations such as Indonesia provide no explicit harm requirement in their laws.[48] The US Espionage Act also does not include a harm requirement. Although courts have interpreted 'respecting the national defense' to mean information that 'would be *potentially damaging* to the United States or *might be* useful to the enemy of the United States',[49] US courts have interpreted the classified status of a document as being sufficient evidence of its potentially damaging nature.[50] Australia's official secrets legislation considers certain information 'inherently harmful', namely classified information or information held, or relating to, any intelligence agency, and a public servant who discloses such information may be convicted of an offence which has no further harm element.[51]

By contrast, other countries, including Cambodia, Serbia and the Philippines include as a necessary condition for criminal liability a showing of damage, or likely damage, resulting from the speech.[52] Article 445 of Cambodia's Criminal Code criminalizes giving or 'facilitating easy access by foreign agents' to information which 'undermines

[45] Singaporean Official Secrets Act. See also Pakistani Official Secrets Act s. 5(c); Ugandan Official Secrets Act of 1964 ch. 302 s. 4. Uganda also criminalizes by separate provision employees of Ugandan 'security organizations' who release or disclose 'any information relating to his or her duties': Ugandan Security Organisations Act of 1987 ch. 305 s. 10.

[46] Australian Criminal Code Act s. 90.1, which defines 'deal'. When a Bill inserting this definition was brought to a parliamentary inquiry, 14 Australian media organizations expressed concern that journalists, editorial, and support staff, would be at significant 'risk of jail time as a result of merely having certain information in their possession in the course of news reporting', including the receipt of unsolicited information and making a record of such information: Joint Media Organisations, 'Submission to the Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017' (22 January 2018).

[47] See, e.g., Turkish Penal Code Arts 327, 329, 330.

[48] Indonesian State Intelligence Act 2011 Arts 44 and 45.

[49] US Court of Appeals, Fourth Circuit, *United States v. Morison* 844 F.2d, 1 April 1988, 1057, 1071 (emphasis added). See also D. McCraw & S. Gikow, 'The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World' (2013) 48 *Harvard Civil Rights-Civil Liberties Law Review* 473, 497.

[50] See, e.g., Feuer (n 7) 126, citing US District Court for the Eastern District of Virginia, *United States v. Kiriakou* No. 1:12cr127 (LMB) 8 August 2012, 1, 15–16.

[51] Australian Criminal Code Act s. 121.1, which defines 'inherently harmful information'. Australia's espionage offences are complex and Australian law also includes other piecemeal disclosure provisions that could be applied to journalists: see S. Kendall, 'Espionage and Press Freedom In Australia' (The University of Queensland, 2020).

[52] Cambodian Criminal Code 2009 Art. 445; Serbian Criminal Code 2005 Art. 316; Philippine Revised Penal Code Act No. 3815 Art. 229.

the national security'.[53] And in some jurisdictions, the existence or degree of harm influences the level of punishment for the disclosure.[54]

The United Kingdom's official secrets laws are mixed as to whether criminal liability requires proof of damage, depending on which category of information is disclosed and who discloses it. No showing of damage is required for disclosures of information 'relating to security or intelligence' by members of the security services, whereas all other individuals (civil servants and members of the public alike) will be liable only when disclosing information that 'causes damage' or 'would be likely to cause' damage, and the definition of damage depends on the nature of the information disclosed.[55]

1.3. Intent

States impose varying standards for mental culpability in laws that penalize disclosures of government material, often addressing two distinct forms of criminal intent: the intent to disseminate the protected information, and the intent to cause harm through the disclosure. As to the first prong, many states such as Norway, Turkey and Indonesia criminalize even the negligent disclosure of state secrets, often as a lower-level offence with reduced penalties.[56] Nations including Denmark and Bolivia provide less severe penalties if disclosure is a result of negligence.[57]

When it comes to the intent to cause harm through the disclosure, some states have expressly provided for a criminal penalty *without* any such intent, effectively creating a strict liability offence for disclosure. For example, Spain's Penal Code criminalizes '[a]nyone who, without intending to benefit a foreign power' discloses legally classified or secret information 'related to national security or national defence or to technical methods or systems used by the Armed Forces or by industries of military interest'.[58] In contrast, a number of states provide explicit intent to harm standards but set a fairly low bar. For instance, the US Espionage Act requires that a defendant who possesses and 'willfully transmits' or 'willfully retains' information relating to the national defence 'has reason to believe' that the information 'could be used to the injury of the United States or to the advantage of any foreign nation'.[59]

Other states require intent to harm, but put in place broad presumptions for the defendant to rebut. For example, section 3(1) of Myanmar's Official Secrets Act criminalizes any person who 'for any purpose prejudicial to the safety and interests' of that state

[53] Cambodian Criminal Code 2009 Art. 445.

[54] See, e.g., Norwegian Penal Code s. 124 (providing a term of imprisonment not exceeding 15 years for the aggravated disclosure of a state secret: 'In determining whether the disclosure is aggravated, particular weight shall be given to whether … (d) considerable harm has resulted'); Georgian Criminal Code Art. 313(2).

[55] UK Official Secrets Act ss 1–6. These offences (with the exception of section 6) also have a corresponding defence of 'not knowing and having no reasonable cause to believe' that the disclosure would be damaging: UK Official Secrets Act ss 1(5), 2(3), 3(4), 4(4), 5(2). See s. II.2.1.1. (United Kingdom).

[56] Indonesian Draft Law Number 17 of 2011 Arts 44–45; Norwegian Penal Code s. 125; Turkish Penal Code Arts 329(3), 338.

[57] See Danish Criminal Code Art. 152; Bolivian Penal Code Art. 115.

[58] Spanish Penal Code Art. 598. The penalty under this provision is one to four years, but Art. 599 provides that the penalty should be applied 'in the upper half' in circumstances where the speaker had knowledge of the information due to his office or post, or the disclosure consists of publicizing the information on social media or 'in a way that ensures its diffusion'.

[59] 18 U.S.C. §793(e).

'obtains … or communicates' 'any secret … information which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy'.[60] Section 3(2) of the legislation then provides that:

> it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety and interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, *from the circumstances of the case of his conduct or his known character as proved,* it appears that his purpose was a purpose prejudicial to the safety or interests of the State.[61]

Bangladesh and Uganda's Official Secrets Acts incorporate the same presumption.[62]

1.4. Exclusions, exceptions and defences

1.4.1. Public interest

Many countries with a reputation for vigorous protection of freedom of the press—notably the United Kingdom and the United States—do not consider the public interest in disclosure of official secrets to be an exception to criminal liability. There are, however, states that do enshrine such a defence in their espionage and official secrets laws to varying degrees.

For example, Denmark's Criminal Code provides an absolute public interest defence for disclosure of confidential information obtained while in public service, holding that state secrets laws 'do not apply in cases where the person in question … acted in order to lawfully safeguard obvious public interests or the interest of himself or other persons'.[63] Slovenia, Canada and Australia incorporate conditional public interest defences in certain circumstances or consider the issue of public interest as a factor in a balancing test. In Slovenia's case, an individual disclosing classified information no longer incurs criminal liability provided that 'the public interest in the disclosure of classified information prevails over the public interest in maintaining its secrecy' and if the disclosure 'does not directly endanger the life of one or more persons'.[64] This legislation was passed following backlash surrounding the prosecution of a journalist who disclosed links between Slovenian political and military officials and neo-Nazi groups.[65]

Canadian law creates a stringent public interest balancing exercise that only applies to a small subset of Canada's official secrets provisions relating to those 'bound to secrecy', making it of limited utility to journalists or other non-state actors.[66] A speaker seeking to argue public interest in disclosure must meet a two-part test: showing that they acted 'for the purpose of disclosing an offence … that he or she reasonably believes has been, is being or is about to be committed by another person in the purported performance

[60] Myanmar Official Secrets Act s. 3(1)(c).
[61] Ibid., s. 3(2) (emphasis added).
[62] Ugandan Official Secrets Act 1964 ch. 302 s. 2(2); Bangladesh Official Secrets Act s. 3(2).
[63] Danish Criminal Code Art. 152 (e). Journalists who obtain or use this confidential information are also protected under Art 152 (d). Not all Danish official secrets laws incorporate a public interest defence: see Danish Criminal Code, Arts 107 (disclosure of secret information to a foreign power or organization), 109 (disclosure of secret information regarding 'secret negotiations, consultations or resolutions of the state in matters affecting the security or rights of the state relative to foreign states or involving substantial economic interests').
[64] Slovenian Criminal Code Art. 260(4).
[65] See s. II.2.1.2. (Slovenia).
[66] Canadian Security of Information Act RSC 1985 c. O-5 s. 15.

of that person's duties and functions for, or on behalf of, the Government of Canada', and that the public interest in the disclosure of this offence outweighs the public interest in non-disclosure.[67] But a strict pre-condition of the latter prong requires showing that the speaker made a prior disclosure to certain government officials or agencies, unless a 'direct' disclosure was necessary to avoid grievous bodily harm or death.[68]

Australia's official secrets laws, on the other hand, include a public interest reporting defence available to 'persons engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media' as well as administrative staff acting under direction at news media entities.[69] This law provides for a defence to the prosecution under official secrecy laws if such a person communicated or dealt with information in their capacity as a person engaged in reporting news and 'at that time, the person reasonably believed that engaging in that conduct was in the public interest'.[70] This provision includes a number of exceptions: a person may not reasonably believe that disclosing or dealing with information is in the public interest if that conduct would involve publication of the identity of an Australian intelligence employee or affiliate, would involve an offence under witness protection legislation or if that conduct was in engaged in 'for the purpose of directly or indirectly assisting a foreign intelligence agency or foreign military organisation'.[71] And media organizations and civil society groups have argued that the defence does not go far enough as it may not cover individual bloggers, and 'does not extend to a journalist's sources, or to civil society groups or advocates, an obvious impediment to political debate and to reporting these kinds of stories'.[72]

Other states provide public interest defences for state officials—and in some circumstances, the wider population—under their laws. For instance, Rwanda and Nigeria include carve-outs in their laws for public interest disclosures related to official wrongdoing, abuse of authority or acts of negligence.[73] Thailand's legislation provides an exemption from liability for disclosures by state officials who act in good faith and disclose information for the purpose of 'securing a benefit of greater importance which relates to public interest, life, body, health or other benefit of a person and such an order is reasonable'.[74]

[67] Ibid., s. 15(2). The provision also provides a number of relevant considerations that must be addressed, including whether the person resorted to reasonable alternatives and the 'nature of the harm or risk of harm created by the disclosure': s. 15(4).

[68] Canadian Security of Information Act RSC 1985 c O-5 s. 15(5). Cf. Canadian Superior Court of Justice of Ontario, *O'Neill v. Canada (Attorney General)* (2006) 82 O.R. (3d) 241, 19 October 2006.

[69] Australian Criminal Code Act s. 122.5(6). However, Australia's public interest offence does not apply to all espionage and official secrets laws that might capture journalistic speech, and a recent Parliamentary Committee has recommended that the 'Government give consideration to whether defences for public interest journalism should be applied to other secrecy provisions': Parliament of the Commonwealth of Australia Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (2020), §3.198.

[70] Australian Criminal Code Act s. 122.5(6). The defendant bears the evidential onus of proof in relation to this defence.

[71] Australian Criminal Code Act s. 122.5(7). See Kendall (n 51) 9.

[72] L. Taylor, 'We need to talk about press freedom before it's too late' (The Guardian Australia, 22 June 2018).

[73] Rwandan Law Relating to Access to Information Arts 4, 16, providing a defence 'if the person believes on reasonable grounds that the information is accurate and the disclosure is in the public interest'. Cf. Rwandan Law Determining Offences and Penalties in General Art. 192; Nigerian Freedom of Information Act s. 27(2) (which provides that nothing in the Criminal Code or Official Secrets Act shall prejudice a public officer who 'without authorisation, discloses to any person' information which he reasonably believes to show mismanagement, fraud, abuse of authority or 'a substantial and specific danger to public health or safety').

[74] Thai Official Information Act 1997 ss 15, 20.

1.5. Penalties

Penalties for violations of espionage and official secrets laws cover a very wide range.[75] Table A shows the spread of *maximum* penalties for official secrets and espionage laws for a range of countries analysed for or mentioned in this chapter.

Table A: Range of Penalties in National Laws[76]

Maximum sentence	Countries
0–4 years	Slovenia
5–9 years	Bolivia, France, Poland
10–15 years	Argentina, Austria, Canada, Germany, Ghana, India, Indonesia, Iran, Japan, Myanmar, Nigeria, Norway, Panama, Peru, Qatar, Serbia, Singapore, Spain, Sri Lanka, United Kingdom
16–25 years	Albania, Belgium, Georgia, Moldova, Rwanda, Zimbabwe
26 years–life	Australia, Cambodia, Czech Republic, Denmark, El Salvador, Hong Kong, Philippines, The Gambia, Malaysia, Turkey
Capital punishment	Bangladesh, Republic of Korea, Pakistan, Thailand, Uganda, United States

[75] The use of injunctive relief to prevent the disclosure of unauthorized information is beyond the scope of this report. The penalties described in this section relate to pure speech offences rather than other, more traditional, spying laws. See s. I. Introduction.

[76] This table is non-exhaustive: Albanian Criminal Code 2017 Art. 213; Argentine Penal Code Art. 222 (lesser penalties apply if the offender is not a member of the military); Austrian Criminal Code Arts. 252, 253, 254; Australian Criminal Code Act s. 91(6) (s. 91(6) penalizes aggravated espionage, however lesser terms of imprisonment apply to other Australian official secrets laws: see Australian Criminal Code Act ss 122.4; 122.4A(1)); Belgian Penal Code Arts. 118, 119 (up to 20 years' imprisonment if committed by a public official or 15 years' imprisonment if committed by a private person); Bangladesh Official Secrets Act 1923 s. 3; Bolivian Penal Code Art. 115; Cambodian Criminal Code 2009 Art. 443; Canadian Security of Information Act s. 27 (although a range of penalties apply under this Act); Czech Criminal Code (2009) ss 316(4), 54 (1); Danish Criminal Code Art. 109 (if information is passed on to a foreign power or if espionage is committed in war time); El Salvador Criminal Code Art. 356 (penalizing espionage, cf. Art. 355 (penalizing disclosure of state secrets by up to 8 years' imprisonment)); French Penal Code Art. 413-10 and Official Secrets Act s. 17; Georgian Criminal Code Art. 314; The Gambia Official Secrets (Amendment) Act 2008 s. 17(1)(a); German Criminal Code ss 95, 96; Ghanaian State Secrets Act 1962 (Act 101) s. 14; Hong Kong National Security Law Arts 20, 22 (penalizing secession or subversion 'of a grave nature', cf. Hong Kong Official Secrets Ordinance s. 25, providing lesser penalties for other violations of official secrets offences); Indian Official Secrets Act s. 3; Indonesian Draft Law No. 17 of 2011 Art. 46; Iranian Islamic Penal Code Art. 501; Japanese Act on Protection of Specially Designated Secrets Arts 23, 24; Korean Criminal Code Art. 98 and National Security Act Art. 4(1), item 2; Malaysian Penal Code s. 124M and Official Secrets Act 1972 s. 3; Moldovan Criminal Code Art. 338; Myanmar Official Secrets Act s. 3 and Myanmar Electronic Transactions Law s. 33; Nigerian Official Secrets Act s. 7; Norwegian Penal Code ss 123, 124; Pakistani Official Secrets Act s. 3 (added by the Official Secrets (Amdt.) Act 1966 (8 of 1966)); Panama Criminal Code Art. 428; Peruvian Criminal Code Arts 330–331; Philippine Act to Punish Espionage and Other Offenses Against the National Security s. 2 (if committed during war time, cf. Philippine Revised Penal Code Art. 117); Polish Penal Code Art. 265(1) (if acting in the name of or on behalf of a foreign entity); Qatari Penal Code Art. 110; Rwandan Law Determining Offences And Penalties In General Art. 192 (applicable in war time); Serbian Criminal Code Art. 316; Singaporean Official Secrets Act s. 17(1); Slovenian Criminal Code s. 260(1); Spanish Criminal Code Art. 584; Sri Lankan Official Secrets Act s. 26(1); Thai Criminal Code s. 124; Turkish Penal Code Arts. 328, 329, 330 (the maximum penalty of life imprisonment applying if the disclosure is 'military espionage'); Ugandan Security Organisations Act (1987) ch. 305 s. 10(1) (applying to employees of security organizations releasing information relating to their duties, cf. Ugandan Official Secrets Act ch. 302 Art. 15 (applying to all persons, punishable by 14 years' imprisonment)); UK Official Secrets Act 1989 s. 10 and Official Secrets Act 1920 s. 8 (providing for up to 14 years' imprisonment for offences under the Official Secrets Act 1911); 18 U.S.C. §794 (gathering or delivering defence information to aid a foreign government); cf. 18 U.S.C. §793 (gathering, transmitting or losing information 'relating to the national defense', punishable by up to 10 years' imprisonment); Zimbabwean Official Secrets Act s. 3.

This range of criminal penalties can equate to very expansive sentences, especially when other offences are said to be involved. For instance, the indictment of Edward Snowden covered three counts, for theft of government property, unauthorized communication of national defence information and wilful communication of classified intelligence information to an unauthorized person, and on this basis could expose him to up to 30 years in prison.[77] In many states, a defendant may also be subject to heavy fines.[78]

Some states set out factors which may aggravate or mitigate penalties when it comes to sentencing. For example, Norway provides for a list of factors to determine whether a disclosure is 'aggravated', such as whether:

> a) the perpetrator is a member of the Government, the Parliament or the Supreme Court, or a member of the country's highest civilian or military leadership, b) the secret was entrusted to the perpetrator in the course of service or work, c) the secret has been disclosed to a foreign state or a terrorist organization, d) considerable harm has resulted.[79]

Australia's Criminal Code includes aggravated offences that increase prescribed penalties for underlying offences. Aggravating circumstances include where the underlying offence was committed in circumstances including dealing with information from a foreign military agency, dealing with five or more security classified records, altering a record to remove or conceal its security classification and holding an Australian government security clearance allowing access to at least 'secret' security classified information at the time the person dealt with the information.[80]

2. Application of Espionage and Official Secrets Laws Around the World

Espionage laws of every stripe have been used across the globe to punish state officials, ordinary citizens and journalists and to deter others from reporting on legitimate stories of public interest at odds with the government's perspective. Cases that showcase key trends, set important precedents, or have prompted significant reforms are outlined below.

2.1. Europe and United Kingdom

2.1.1. United Kingdom

The British case of Clive Ponting, although dated, reflects the challenges of official secrets laws that are devoid of a public interest defence.[81] Ponting, an employee at the

[77] S. Shane, 'Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance' (The New York Times, 21 June 2013).
[78] See, e.g., UK Official Secrets Act 1989 s. 10; French Penal Code Art. 413-10; French Official Secrets Act s. 17 (100,000 EUR).
[79] Norwegian Penal Code ch. 17 s. 124.
[80] Australian Criminal Code Act ss 91.6, 122.3.
[81] UK Central Criminal Court, *R. v. Ponting* 1985 Crim L.R. 318, 11 February 1985.

UK Ministry of Defence, admitted to disclosing classified documents to a Member of Parliament about the sinking of an Argentine warship during the Falklands conflict in 1985.[82] Prior to the disclosure, Prime Minister Margaret Thatcher had told Parliament that the warship had been steaming towards, and therefore threatening, the British Royal Navy, and on that basis she had accepted a naval commander's request to sink the ship despite over 1,000 sailors being onboard.[83] However, Ponting uncovered information that suggested that the ship was in fact steaming *away* from the British, and after being told by his superiors to keep quiet, Ponting reported this to one of Thatcher's opponents, Labour MP Tam Dalyell.[84]

Ponting was charged under section 2(1) of the Official Secrets Act 1911, which provided that it was an offence to communicate any official information to a person other than 'a person to whom it is in the interest of the State his duty to communicate it'.[85] The law did not include an explicit public interest defence.[86] At his trial, Ponting argued that the phrase 'in the interests of the State' amounted to an implicit public interest defence and submitted that, in communicating the impugned information to Dalyell, he had acted in the public interest—which, he made clear, need not be the same as the interests of the government of the day.[87] The judge disagreed with this construction, summing up to the jury as follows:

> What, then of the words, 'the interests of the state'? Members of the jury I direct you that those words mean the policies of the state as they were in July 1984 when Mr Pointing communicated the information to Mr Dalyell, and not the policies of the state as Mr Ponting, Mr Dalyell, you or I might think they ought to have been … I direct you in law that it is no defence that he honestly believed that it was his duty to leak the documents in the interests of the state if, in fact, it was not his duty to do so in the interests of the state.[88]

Despite this direction, the jury acquitted Ponting.[89] The case led to a debate as to whether, and if so how, the Official Secrets Act should be reformed. A private members Bill which included an explicit public interest defence was introduced, and defeated, in 1988. The British Government ultimately passed the Official Secrets Act 1989, which amended the 1911 Act but did not incorporate a public interest defence. The government of the day argued at the time that 'it cannot be acceptable that a person can lawfully disclose information which he knows may, for example, lead to

[82] M. Rosenbaum, 'Clive Ponting case: Where is the investigators' report?' (BBC News, 18 May 2011).

[83] P. Davison, 'Clive Ponting, British defense official who turned whistleblower, dies at 74' (The Washington Post, 11 August 2020).

[84] Ibid.

[85] UK Official Secrets Act 1911 s. 2: see Bartlett & Everett (n 3) 12–13, 42.

[86] However, an earlier version of the same offence, section 2 of the UK Official Secrets Act 1889, did explicitly reference the public interest, prohibiting breaches of official trust, but only those contrary to the 'interests of the State' or 'the public interest'. The 1911 Act was passed after successive attempts to tighten the 1889 law, which British governments considered weak and difficult to prosecute as it only applied to Crown Servants and government contractors and when a communication was *not* in the public interest.

[87] Rosenbaum (n 82).

[88] Bartlett & Everett (n 3) 5.6.

[89] D. Hewitt, ' "Not only a right, but a duty": A history of perverse verdicts' (The Justice Gap, 1 May 2018).

loss of life simply because he conceives that he has a general reason of a public character for doing so'.[90]

However, the Law Commission of England and Wales has since called for the introduction of such a defence in English law[91] on the basis that it was 'unable to state with confidence' that the current law on unauthorized disclosures 'afford[ed] adequate protection to Article 10 rights' protecting freedom of expression.[92] The Commission considered that a reasonable belief that the disclosure was in the public interest was insufficient and that to benefit from this defence the speaker must prove,[93] on the balance of probabilities, that the subject matter of the disclosure, and the manner in which it was disclosed, were in the public interest.[94] The Commission considered making a public interest defence available for journalists or those engaged in 'journalistic activity', similar to Australia's legislation and the UK Data Protection Act. Although it did not reach a clear conclusion on this point,[95] it considered it 'important to note' that European case law 'does not depend on the definition of "journalist" '.[96]

The Law Commission report also recommended expanding the territorial ambit of the United Kingdom's espionage provisions,[97] removing the requirement to prove

[90] L. Maer & O. Gay, 'Official Secrecy' (UK House of Commons Library, 30 December 2008), 2, 3, 6; A. Bailin, 'Let's free the Official Secrets Act from its cold war freeze' (The Guardian, 22 September 2011).

[91] The public interest defence recommended by the Commission has two components. For public servants, the Commission recommended that a statutory commissioner be established, and that there should be a 'strong presumption' of disclosure to the commissioner, although a public interest defence would nonetheless be available. For non-public servants, the Commission considered that the defence should be available to anyone charged under the Official Secrets Act 1989. UK Law Commission, *Protection of Official Data Report* (2020), §§9.153, 10.71. The Commission recommended some minimum requirements for such a statutory commissioner: independence, the ability to meaningfully investigate allegations, compel cooperation with investigation and act expeditiously and incorporate a right to appeal against its decisions: §§10.108–10.110.

[92] Ibid., §§9.6, 11.13–14 (citing the ECHR's *Bucur and Toma v. Romania* case and noting that such a defence would 'increase the likelihood' of compliance with article 10 'in all situations', as it 'provides a backstop in the event that the mechanisms for investigation and redress are rendered ineffective'); UK Law Commission, '*Protection of Official Data: Summary*' (2020), 9. See s. III.4 (Necessity).

[93] UK Law Commission, *Protection of Official Data Report* (2020), §11.79. Although it considered whether only an evidential burden should lie with the defence (whereby 'the defence must raise an issue of public interest sufficient for the prosecution to disprove it as part of the burden of proof resting on the prosecution'), the Commission ultimately favoured a more stringent 'persuasive burden', whereby the defendant must show on the balance of probabilities that the disclosure was in the public interest: §§11.28–11.34. The Commission considered the former formulation might place 'impossible demands on the prosecution', require extensive disclosure of information and was not unduly challenging for the defence as it was only a balance of probabilities burden: §§11.31, 11.34.

[94] UK Law Commission, *Protection of Official Data Report* (2020), §11.28. The Commission considered whether the public interest should be a 'subject matter' approach, in which a disclosure would only be considered in the public interest if it fell within certain categories of information: §§11.54–11.59. However, the Commission preferred a broader approach consistent with Canadian law, whereby legislation provides types of disclosures that are *not* in the public interest as well as a list of factors which are relevant to whether the disclosure *is* in the public interest: §§11.60–11.66, 11.76–11.81.

[95] Ibid., §§11.67–11.75.

[96] Ibid., §§11.70. The Commission's recommendation to implement a public interest defence only extends to offences under the Official Secrets Act 1989 and not to espionage offences. The Commission argued that 'to be guilty of espionage, an individual would have to act with a purpose they knew or had reasonable cause to believe was prejudicial to the interests of the state' and as such 'is not commensurate with a public interest defence': UK Law Commission, '*Protection of Official Data: Summary*' (2020), 10.

[97] UK Law Commission, *Protection of Official Data Report* (2020), §§3.150–3.152. The Commission also recommended that the territorial ambit of ss 1–4 of the Official Secrets Act 1989 should be amended so that offences of disclosure by government contractors apply irrespective of whether he or she is a British citizen, in effect expanding the territorial application of that Act: §5.222.

damage from certain unauthorized disclosure provisions[98] and increasing maximum[99] penalties.[100] These recommendations were strongly opposed by a number of media organizations and civil rights groups. But the Commission considered that such concerns 'will have been addressed by fortifying and balancing this recommendation' with its most significant proposed amendment: the inclusion of a public interest defence for those charged under the Official Secrets Act 1989.[101]

In a consultation paper published in 2021 following the Law Commission's report, the UK Home Office stated that it disagreed with the proposal for a public interest defence, observing that it 'believes that existing offences are compatible with Article 10 and that these proposals could in fact undermine our efforts to prevent damaging unauthorized disclosures, which would not be in the public interest'.[102] The government also argued that a whistleblower will 'rarely (if ever) be able to accurately judge whether the public interest in disclosing the information outweighs the risks against disclosure'.[103] The Home Office sought consultation on its own set of recommendations, focused on adopting some of the Law Commission's stricter provisions[104] while disregarding the balancing it recommended through a public interest defence.[105] The National Security Act, sponsored by the Home Office and enacted into law in July 2023, includes a reform

[98] The current Act requires proof that the disclosure caused, or was likely to cause, damage to a specific state interest before primary disclosures (by public officials) and secondary disclosures (by members of the public, including journalists) will be unlawful (except for certain information disclosed by a member of the security and intelligence services). However, the Commission recommended that damage only need be proved for secondary disclosures, rather than primary disclosures by public officials. The rationale behind this recommendation was that the 'damage requirement presented a practical hurdle for prosecutors who would be required to disclose further sensitive information at trial'. See UK Law Commission, *Protection of Official Data Report* (2020), §§4.80–4.83, 4.14–4.15.

[99] Ibid., §§5.47, 5.55, 5.70–5.72. The Commission described the existing two-year maximum sentence under the Official Secrets Act 1989 as 'low when compared to the maximum available sentence in similar jurisdictions', for example Canada's Security and Information Act 2001, which provides a 14-year maximum. Guardian News and Media questioned the validity of this assertion, noting that many countries limit the maximum sentence to five years' imprisonment absent proof of delivery of information to a foreign state or intent to prejudice security or defence. The Commission did not specify what the maximum sentences should be, but noted that a distinction should be made between offences committed by civil servants versus others. The UK Government has supported all but the final component of the Commission's recommendation on penalties, and asked consultees whether there should be such a distinction. UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (2021), 19–20.

[100] It also proposed updating some 'archaic' language in the Official Secrets Act 1911 and 1920. See UK Law Commission, *Protection of Official Data Report* (2020), §§3.32, 3.110 (such as replacing references to 'sketch, plan, model, note . . . ' with 'document, information or other article', and replacing 'enemy' with 'foreign power').

[101] Ibid., §4.80. The United Kingdom has previously had some form of a public interest defence in that a criminal sanction for a breach of official trust was limited to breaches which could be shown to be contrary to the public interest. Section 2(1) of the Official Secrets Act 1889 prohibited communication of information to any person to whom it 'ought not, in the interest of the State, or otherwise in the public interest' to be communicated. This was repealed and replaced by a more narrow provision in section 2 of the Official Secrets Act 1911, which again was repealed with the passage of the Official Secrets Act 1989: see Bartlett & Everett (n 3) 12–13, 19–21.

[102] UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (2021), 24. See s. IV. (Recommendations).

[103] Ibid.

[104] The UK Government welcomed the proposal to remove the harm requirement, noting 'that both primary and onward disclosures have the potential to cause equal amounts of harm' and has requested consultation as to whether this proposal should be extended even further, to secondary disclosures: UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (2021) 18. This sits in contrast to the Law Commission, which was at pains to distinguish primary and secondary disclosures on the basis that 'concerns about over-criminalising conduct that is not causing damage are quite different' in each case: UK Law Commission, *Protection of Official Data Report* (2020), §§4.13, 4.34; 4.43.

[105] UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (2021), 24.

of espionage offences under the Official Secrets Acts 1911–1939.[106] While the Home Office maintains that the Act 'does not replace' the offences of unauthorized disclosure under the Official Secrets Act 1989,[107] journalists have expressed concern that the new offences 'risks lumping in investigative journalists, whistleblowers and civil-society groups with spies' and lamented the absence of a statutory public interest defence.[108]

2.1.2. Slovenia

In Slovenia, recent amendments to official secrets laws to incorporate a public interest defence were introduced into law following backlash against the attempted prosecution of investigative journalist Anuška Delić. Delić, a reporter for Slovenian newspaper Delo, published a series of articles ahead of Slovenia's 2011 elections revealing connections between a neo-Nazi group 'Blood & Honour' and members of the major political party which ultimately succeeded in forming government.[109]

The Slovenian Intelligence and Security Agency (SOVA) charged Delić under article 260 of Slovenia's Criminal Code with dissemination of classified information, punishable by up to three years' imprisonment. The indictment alleged that Delić's articles contained classified information acquired from an unidentified SOVA official and that she had compromised SOVA's methods by publishing the information.[110]

At trial, Delić gave evidence that the articles contained information already in the public domain and that, in any event, it did not harm SOVA or Slovenia's interests. For example, Delić argued that her sources included Facebook posts which identified the leader of the Blood and Honour group, as well as publicly available registers.[111] And the materials at trial included an internal SOVA report conceding that the agency had not suffered negative consequences as a result of the articles in question.[112] On 15 April 2015, moments before judgment was set to be handed down, state prosecutors withdrew all charges against Delić, but maintained her guilt in a statement before the judge and media.[113]

The case became a catalyst for reform: in October 2014, Slovenia's then Prime Minister said that the case demonstrated 'the need to consider legislation on media freedom', and that '[j]ournalists must be protected from criminal liability for publishing information that is in the public interest'.[114] And in July 2015, Slovenia's parliament

[106] See UK National Security Bill 2022. See also UK Home Office, 'Policy paper—New espionage offences: fact sheet' (13 July 2023) (noting that '[e]spionage is now addressed by 3 offences in the Bill: obtaining or disclosing protected information; obtaining or disclosing trade secrets; and assisting a foreign intelligence service' and that '[t]he Bill repeals the Official Secrets Acts 1911, 1920 and 1939, which contain the existing provisions').

[107] UK Home Office, 'Policy paper—Journalistic freedoms: National Security Bill factsheet' (13 July 2023).

[108] See, e.g., The Editorial Board, 'Another threat to media freedom' (Financial Times, 29 January 2023).

[109] M. Nazar, 'Slovenia: How a neo-Nazi exposé almost landed a journalist in jail' (Index on Censorship, 17 February 2016).

[110] See also R. Greenslade, 'Slovenian journalist facing jail for revealing party's neo-Nazi links' (The Guardian, 15 September 2014).

[111] European Federation of Journalists, 'EFJ demands Slovenian authorities to drop charges against journalist' (4 August 2015).

[112] M. Nazar, 'Slovenia: How a neo-Nazi exposé almost landed a journalist in jail' (Index on Censorship, 17 February 2016). But the report also included a handwritten note from a high-ranking senior official requesting a further report be drafted with a different result, which the prosecution did not produce.

[113] Ibid.

[114] M. Cerar, Tweet 1/2 of 14 October 2014; M. Cerar, Tweet 2/2 of 14 October 2014.

voted 86–1 to introduce a public interest defence for all persons charged under article 260.[115] Although this defence remains in place, Slovenia has experienced a 'swift downturn in press and media freedom' by other means after the Slovenian Democratic Party, the subject of Delić's investigations, returned to power in March 2020, with the International Press Institute reporting extensive social media attacks on journalists and attempts to defund and discredit the state's public broadcaster.[116]

2.2. Asia Pacific

2.2.1. Myanmar

In Myanmar, colonial-era secrecy laws have been used to crack down on journalists and human rights defenders critical of the government. A striking example is the case of Reuters journalists Wa Lone and Kyaw Soe Oo, who were arrested and charged in 2017 under the Official Secrets Act for possessing classified documents containing information about police personnel, arms and ammunition, and attacks in the Rakhine area of Myanmar.

The journalists were convicted despite evidence that the information in the documents was already public, that neither journalist had shared or published the information and that the documents had been planted on them by the police. One police officer, who testified for the prosecution, shocked observers by telling the court that he was present at the meeting at which a police brigadier instructed subordinates to plant the documents on Wa Lone and arrest him.[117] Evidence at trial showed that the true motive for the arrest was the journalists' investigation into the executions of Rohingya Muslims in a village called Inn Dinn in Rakhine State.[118]

The defence centred on evidence that Wa Lone and Kyaw Soe Oo had been lured into a restaurant and had documents planted on them, and that the prosecution had failed to prove the key elements of the charge. First, the prosecution had failed to prove that the documents had been published or shared. Second, there was no evidence the documents were in fact secret, since they were either non-substantive or already in the public domain. Finally, the prosecution had not shown that the documents were intended to be useful to any 'enemy', or that Wa Lone and Kyaw Soe Oo had acted for 'any purpose prejudicial to the safety and interests of the state'.

[115] Slovenia Criminal Code, Art. 260(4). See II.1.4.1. (Public interest); International Press Institute, 'Slovenia introduces public interest defence for those who publish classified information' (IFEX, 21 July 2015). However, Slovenia has retained other misdemeanour offences for disclosure of classified information by persons entrusted with such information which do not incorporate a public interest defence: Slovenian Classified Information Act Arts 44, 44a and 45.

[116] J. Wiseman, 'New Administration, Old Agenda: Press Freedom Strained Again in Slovenia Under Veteran PM Janša' (International Press Institute, 1 September 2020). According to Reporters Without Borders, '[a] climate of hostility toward journalists has defused since Prime Minister Janez Janša's departure in 2022 and the legal framework protecting press freedom remains strong. But the media continues to face political pressure': Reporters Without Borders, 'Slovenia'.

[117] R. Paddock & others, 'Who Was Most Opposed to Freeing 2 Reporters in Myanmar? Aung San Suu Kyi' (The New York Times, 10 May 2019).

[118] Section 3 of Myanmar's Official Secrets Act prohibits the conduct of a person who 'obtains, collects, records or publishes or communicates to any other person any secret official … document or information' that may be 'useful to an enemy'.

Nevertheless, in September 2018, both men were found guilty and sentenced to seven years' imprisonment. The Court held that it was the defendants' responsibility to prove their innocence, refused to accept any exculpatory evidence and considered the documents found on the defendants' phones to contain 'security sensitive matters' which could 'serve as useful information to' armed 'insurgent groups' if it got into their hands.[119] A few months later, the High Court of Yangon Region dismissed the journalists' appeal, focusing on section 3(2) of the Official Secrets Act which provides that it is not necessary to prove a prejudicial purpose if 'from the circumstances of the case' or a defendant's 'conduct or his known character as proved, it appears' that he had such a purpose. The High Court considered that since Wa Lone had tried to meet victims of the Inn Dinn attack, had a notebook allegedly containing phone numbers of members of the Arakan Army, had contacted the officer in question and been in possession of the impugned documents, the prosecution had proved a prejudicial purpose. Myanmar's highest court, the Supreme Court, rejected a further appeal in April 2019.[120]

International outcry followed these decisions. The UN High Commissioner for Human Rights at the time, Michelle Bachelet, stated that the verdict 'sends a message to all journalists in Myanmar that they cannot operate fearlessly, but must rather make a choice to either self-censor or risk prosecution'.[121] Both men were awarded the Pulitzer Prize for their journalism and were ultimately released and relocated abroad.[122]

Since the February 2021 *coup d'etat* in the country, the military junta has charged the country's de facto head of government, Aung San Suu Kyi, and her advisors under the same official secrets laws that were used to convict the 'Reuters two'.[123] In September 2022, Aung San Suu Kyi was convicted and sentenced to three years' imprisonment for this crime.[124]

2.2.2. Australia

In two recent cases, the Australian Federal Police (AFP) conducted raids as part of its investigations into the unauthorized disclosure of classified information.[125] In June 2019,

[119] Yangon Northern District Court, *Police Lieutenant Colonel Yu Naing v. Thet Oo Maung (Wa Lone) and Kyaw Soe Oo (Moe Aung),* 3 September 2018 (unofficial translation).

[120] S. Naing & S. Lewis, 'Myanmar's top court rejects final appeal by jailed Reuters journalists' (Reuters, 23 April 2019).

[121] OHCHR, 'Comment by UN High Commissioner for Human Rights Michelle Bachelet on the conviction of two Reuters journalists in Myanmar' (3 September 2018).

[122] The Pulitzer Prizes, 'Staff of Reuters, with notable contributions from Wa Lone and Kyaw Soe Oo' (8 February 2018); J. van Leuven, 'Wa Lone and Kyaw Soe Oo honored with the Pulitzer Prize' (Deutsche Welle, 17 April 2019). Following pressure from civil rights groups and diplomatic channels, and after almost a year and a half behind bars, Wa Lone and Kyaw Soe Oo were released in May 2019 as part of a presidential amnesty for 6,520 prisoners. S. Lewis & S. Naing, 'Two Reuters reporters freed in Myanmar after more than 500 days in jail' (Reuters, 7 May 2019).

[123] 'Myanmar: Aung San Suu Kyi charged with violating secrets law' (BBC, 2 April 2021).

[124] This is one of many cases against Suu Kyi, who was sentenced to a total of 33 years in prison: 'Court rulings against Myanmar's Aung San Suu Kyi' (Reuters, 30 December 2022). In August 2023, the military junta announced a partial pardon of Suu Kyi, reducing her 33-year sentence by six years: C. Hall, 'Myanmar Supreme Court dismisses appeals of Aung San Suu Kyi corruption convictions' (JURIST, 6 October 2023).

[125] Australia does not have a right to freedom of speech that is generally understood as a 'personal' or 'individual' right like freedoms conferred by a Bill of Rights in the American model. Rather, Australian courts have held that provisions of the Australian Constitution that created a system of representative government gave rise to an 'implied' freedom to discuss political and governmental affairs. See High Court of Australia, *Lange v Australian*

the AFP conducted a search at the home of News Corp journalist Annika Smethurst, after Smethurst published allegations that the Australian Government had considered a proposal to expand programs to spy on Australian citizens without warrants.[126]

Within a day of the Smethurst raid, the AFP conducted a second raid, this time at the Sydney headquarters of Australia's public broadcaster, the Australian Broadcasting Commission (ABC). The raid concerned reports known as the 'Afghan Files', published nearly two years earlier by journalists Dan Oakes and Sam Clark. The reports alleged the unlawful killing of Afghan civilians by Australian special forces soldiers, revealed by way of 'hundreds of pages of secret defence force documents leaked to the ABC'.[127] The search warrant was issued under section 3E of the Crimes Act 1914, and named Mr. Oakes and whistleblower and former military lawyer David McBride. The raids prompted significant public outcry from journalists and human rights advocates,[128] with The New York Times' Editorial Board describing the raids as 'straight from the playbook of authoritarian thugs'.[129]

Both warrants were challenged in court. Smethurst was successful on narrow grounds in what was described as a 'pyrrhic victory' for press freedom,[130] and the ABC's challenge failed.[131] In rejecting the ABC's grounds for challenging the warrant, Justice Abraham dismissed the argument the AFP's conduct may have a chilling effect on prospective whistleblowers, noting 'that the US doctrine of "chilling effect" has no place in the Australian constitutional context'.[132] The ABC's Managing Director announced that the broadcaster would not appeal the decision, stating 'we don't believe we can litigate our way to reforming fundamentally bad laws'.[133]

Despite the raids, Australian prosecutors ultimately declined to follow the AFP recommendation to charge Mr. Oakes, stating that they had 'determined the public interest does not require a prosecution in the particular circumstances of the case'.[134]

Broadcasting Corporation [1997] HCA 25; (1997) 189 CLR 520, 8 July 1997; High Court of Australia, *McCloy v New South Wales* [2015] HCA 34; (2015) 257 CLR 178, 07 October 2015.

[126] Smethurst published details of a proposal to allow the Australian Signals Directorate (ASD) to secretly access the communications, bank records and other materials of Australian citizens with ministerial authorization.

[127] D. Oakes & S. Clark, 'The Afghan Files: Defence leak exposes deadly secrets of Australia's special forces' (ABC News, 10 July 2017).

[128] See, e.g., M. Ketchell, 'Australia doesn't protect free speech but it could' (The Conversation, 6 June 2019); A. Galloway, 'A chilling effect': Human Rights Watch slams Australia's raids on the media' (Sydney Morning Herald, 15 January 2020); Amnesty International, 'Response to AFP raids on Australian Press' (5 June 2019).

[129] 'Why Are the Australian Police Rummaging Through Journalists' Files?' (The New York Times, 6 June 2019).

[130] Due to errors on the face of the warrant, none of the seven High Court judges that ruled on the matter thought it necessary to answer a much anticipated question on infringement of the implied freedom of political communication: D. Levitan & D. Hurley, 'Memo from our lawyers to journos everywhere: Smethurst's win is a pyrrhic victory for freedom' (Crikey, 17 April 2020); High Court of Australia, *Smethurst v. Commissioner of Police* [2020] HCA 14; (2020) 376 ALR 575, 15 April 2020.

[131] Federal Court of Australia, *Australian Broadcasting Corporation v. Kane (No. 2)* [2020] FCA 133, 17 February 2020.

[132] Ibid., §231, citing High Court of Australia, *Brown v. Tasmania* [2017] HCA 43; (2017) 261 CLR 328, 18 October 2017, at [262] per Nettle J.

[133] 'ABC statement on Federal Court ruling' (ABC, 28 February 2020).

[134] As quoted by the AFP, 'AFP statement on investigation into ABC journalist' (15 October 2020). Sam Clark, the producer of the program, was cleared by the AFP of any potential charges in July 2020: see 'Journalists express concerns as AFP recommends charges against ABC Reporter' (SBS News, 3 July 2020). In November 2020, the Inspector-General of the Australian Defence Force released the results of an inquiry into the Australian special

The investigation against Smethurst was also dropped.[135] Journalists and human rights advocates have argued that nevertheless the chilling impact of the AFP's actions has fundamentally impacted Australia's media environment, and the episode led to two parliamentary inquiries reviewing the relevant laws.[136]

2.2.3. Cambodia

The arrest and trial of Cambodian journalists Yeang Sothearin and Uon Chhin is an example of a vague state secret law being used to harass journalists and criminalize speech that is neither secret nor harmful. In 2017, Yeang Sothearin and Uon Chhin, two journalists who had worked for Radio Free Asia, were charged with committing an 'act of giving or facilitating easy access by a foreign state or its agents, to information … which undermine[s] the national defence'.[137] The Cambodian government claimed that one of the journalists took broadcasting equipment from the Radio Free Asia bureau, installed it in a private residence and the journalists then used this equipment to continue to transmit reports to Radio Free Asia's Washington D.C. Headquarters.[138] These charges came one month after Cambodian authorities ordered the closure of 32 radio frequencies, particularly stations that relayed independent Khmer language news broadcasts.[139] After the closure of the Radio Free Asia bureau, senior officials from the government threatened that any journalists still filing media reports would be labelled as spies.[140]

Uon Chhin and Yeang Sothearin admitted to sharing publicly available information about local events with Radio Free Asia but denied having undermined national security in any manner.[141] At trial, the prosecution was not able to identify any information disclosed by the defendants that was not publicly available at the time of the alleged disclosure and failed to explain the impact of any alleged transmissions on Cambodia's national security.[142] Instead, they simply alleged that the defendants were making the

forces' conduct in Afghanistan, which found credible information of 23 incidents of war crimes committed by Australian personnel: Inspector-General of the Australian Defence Force, *Afghanistan Inquiry Report* (2020), 28–29. However, charges against whistleblower David McBride, a former military lawyer who was named in the search warrant against the ABC as the source of the leaked information regarding war crimes in Afghanistan, have not been dropped. See C. Knaus, 'Defence whistleblower David McBride to stand trial four years and eight months after being charged' (The Guardian, 13 April 2023).

[135] J. Hayne, 'AFP will not lay charges against Annika Smethurst over publishing of classified intelligence documents' (ABC News, 26 May 2020).

[136] See, e.g., S. Ludlam & D. Paris, 'Breaking: A report on the erosion of press freedom in Australia' (Digital Rights Watch, 2019); 'ABC raid: Outcry as Australian police search public broadcaster' (BBC, 5 June 2019); Parliament of Australia, 'Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press: Terms of Reference'; Parliament of Australia, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (2020).

[137] Cambodian General Provisions for Implementation of Criminal Code, Art. 445.

[138] P. Cobus, 'Cambodian Appeals Court Rejects RFA Reporters' Motion for Dismissal' (Voice of America, 29 January 2020).

[139] Ibid.

[140] Editorial Board, 'In Cambodia, journalism has become a crime' (The Washington Post, 23 August 2019).

[141] See G. Sluiter, 'Cambodia vs. Uon Chhin and Yeang Sothearin' (American Bar Association, CFJ, January 2020).

[142] Ibid.

information known abroad, rather than just available in Cambodia.[143] The trial was also tainted by a number of abuses of process.[144]

In October 2019, the Phnom Penh Municipal Court of First Instance ultimately ruled that there was insufficient evidence to convict Uon Chhin and Yeang Sothearin.[145] But instead of dismissing the case, the court sent it for reinvestigation without stipulating a timeline for completion.[146] In 2020, the journalists' appeal to reverse the court's decision to re-investigate their case was rejected by the Court of Appeal and the Supreme Court respectively.[147] Both journalists continue to be on bail and face constraints on their freedom of movement while under judicial supervision.[148]

2.2.4. Hong Kong and China

On 30 June 2020, Chinese authorities passed a draconian 'National Security Law' described as 'Beijing's most aggressive assault on Hong Kong people's freedoms since the transfer of sovereignty in 1997'.[149] The National Security Law criminalizes secession, subversion, terrorist activity and 'collusion with a foreign country' in a manner that is so broad and imprecise that it appears to be capable of capturing any speech critical of the government, wherever uttered at any time in perpetuity.[150] The penalty for secession or subversion 'of a grave nature' is a minimum 10 year prison sentence or a maximum of life imprisonment.[151] And the Law provides that trials 'involving State secrets or public order' can be partially or entirely closed to the public.[152]

The chilling impact of the National Security Law was quickly felt by Hong Kong's press and population. The day after it was passed, over 370 protesters were arrested by police in Hong Kong under its provisions, including for waving independence flags.[153] The following month, over 200 police officers raided the offices of a major pro-democracy newspaper in Hong Kong and arrested and charged its owner Jimmy Lai with 'incitement' and 'colluding with foreign elements'.[154]

[143] Ibid., 26.

[144] Ibid. In 2018, WGAD held that both journalists' right to freedom of expression had been violated and that the 'appropriate remedy' would be to release both men unconditionally and accord them an enforceable right to compensation and reparations: WGAD, *Chhin v. Cambodia* (Opinion no. 3/2019), 24 April 2019, §§64–66.

[145] Human Rights Watch, 'Cambodia: Drop Charges Against Journalists' (19 January 2020).

[146] G. Sluiter, 'Cambodia vs. Uon Chhin and Yeang Sothearin' (American Bar Association, CFJ, January 2020).

[147] UN Secretary-General, *Report of the Secretary General on the Role and achievements of the Office of the United Nations High Commissioner for Human Rights in assisting the Government and people of Cambodia in the promotion and protection of human rights* (2021) UN Doc. A/HRC/48/49, §20.

[148] Human Rights Watch, 'Cambodia: Drop Charges Against Journalists' (19 January 2020).

[149] Human Rights Watch, 'China: New Hong Kong Law a Roadmap for Repression' (29 July 2020).

[150] The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (Hong Kong National Security Law) Arts 20–30. See Amnesty International, 'Hong Kong's national security law: 10 things you need to know' (17 July 2020).

[151] Hong Kong National Security Law Arts 20, 22.

[152] Ibid., Art. 41.

[153] H. Davidson & L. Kuo, 'Hong Kong: hundreds arrested as Security law comes into effect' (The Guardian, 1 July 2020).

[154] Human Rights Watch, 'China/Hong Kong: Mass Arrests Under Security Laws' (11 August 2020); 'Jimmy Lai appears in Hong Kong court in metal chain' (Al Jazeera, 12 December 2020); 'United Nations experts raise concerns with China that proceedings against Jimmy Lai violating his fundamental rights' (Doughty Street Chambers, 31 May 2023); Lai remains in prison awaiting trial, scheduled to begin in December 2023: D. De Luce & J. M. Frayer, 'Jimmy Lai's son says the jailed Hong Kong media tycoon "refuses to be cowed"' (NBC News, 26 September 2023).

The ramifications of the National Security Law in Hong Kong are indicative of a broader crackdown on speech in China ostensibly on the basis of national security concerns. China has been the one of the most prolific jailers of reporters in the world for several years, according to the Committee to Protect Journalists,[155] and prominent journalists have recently been detained under security laws.[156] For example, in August 2020, at a time of increasing tensions between China and Australia, Cheng Lei, an Australian journalist and the face of China's state-run English news service, suddenly disappeared and was charged with 'illegally supplying state secrets overseas'.[157] Chinese authorities also detained a popular Chinese-Australian human rights blogger and charged him with espionage,[158] even though the then Australian Prime Minister decried the allegations as 'absolutely untrue'.[159]

2.3. Middle East and Africa

2.3.1. Iran

A case that illustrates Iranian authorities' pretextual use of espionage offences, alongside fair trial violations and inhumane conditions of detention, is that of Jason Rezaian, a journalist for The Washington Post. Rezaian is a dual American-Iranian national who worked as The Washington Post's Tehran bureau chief from 2012. In 2014, Rezaian and his wife Yeganeh Salehi, also a journalist, were apprehended at their apartment by agents of the Iranian Revolutionary Guard Corps who produced an arrest warrant issued by the Revolutionary Court, which hears alleged crimes relating to national security.[160] The agents forced entry into their apartment, confiscated their passports and electronic equipment and demanded passwords for their social media and email accounts. Both journalists were blindfolded and sent to Evin Prison in Tehran. Salehi was released on bail after approximately 60 days in prison. But Rezaian was ultimately detained for 544 days, and was subjected to long periods of solitary confinement, death threats, sleep deprivation and lack of medical care.[161]

[155] CPJ, 'Number of journalists behind bars reaches global high' (9 December 2021).

[156] J. Griffiths, 'Detention of CGTN anchor shows that in Xi Jinping's China, not even the propagandists are safe' (CNN Business, 1 September 2020).

[157] Ibid.; D. Mendoza, 'Australian Journalist Arrested By Chinese Authorities On Espionage Charge' (OWP, 1 March 2021). See also F. Mao, 'Cheng Lei: Why has an Australian TV anchor been detained by China?' (BBC, 9 September 2020). Cheng Lei was released in October 2023 after serving three years in prison: B. Doherty, H. Davidson & D. Hurst, ' "Tight hugs, teary screams": Cheng Lei releases first statement after release from detention in China' (The Guardian, 11 October 2023).

[158] B. Doherty, 'Yang Hengjun: Australian writer held in China for almost two years officially charged with espionage' (The Guardian, 9 October 2020). Hengjun's trial was held in May 2021 but as of August 2023, he had still not received a verdict or sentence: B. Doherty & R. Touma, 'Detained Australian writer fears he may die of kidney condition in China jail' (The Guardian, 27 August 2023).

[159] Ibid. In a September 2020 consular meeting, the first time anyone outside China's justice system had seen Yang in months, Yang maintained his innocence and stated he had endured more than 300 interrogations and was totally isolated without calls or correspondence in an attempt to 'break him'.

[160] WGAD, *Rezaian v. Iran* (Opinion no. 44/2015), 3 December 2015, §7.

[161] WGAD, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Special Rapporteur on the situation of human rights defenders, UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, UN Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, *Letter to the Representative of the Islamic Republic of Iran*, Reference No. IRN 13/2015, 12 August 2015; US District Court for the District of Columbia, *Rezaian v. Iran* Civil Case No. 16-1960, Memorandum Opinion, 21 November 2019 and Complaint, §50.

Although the Revolutionary Court did not publicly disclose the charges against Rezaian, his lawyer—who 'is believed to be the only person outside the judiciary to have read the indictment'—has stated that Iranian authorities laid four charges, including espionage, collaborating with hostile governments, collecting and distributing information about foreign policies with malicious intent and propaganda against the establishment of Iran.[162] The Iranian Government purportedly relied on two pieces of evidence to sustain these charges: an unsolicited and unsuccessful job application to join the Obama-Biden 'transition team' in 2008, and correspondence between Rezaian and US officials in Dubai, where Rezaian requested his wife's visa process to be expedited as 'sometimes [Iran is] not the best place to be a journalist'.[163]

Following a trial marred with due process violations,[164] the Iranian authorities announced that Rezaian had been found guilty of espionage and sentenced to an unspecified prison term.[165] Rezaian was ultimately released as part of a prisoner swap in January 2016, following extensive public outcry about the case[166] and a decision by the UN Working Group on Arbitrary Detention finding that his detention was arbitrary and a violation of his right to freedom of expression.[167] Rezaian and his family members have since succeeded in a claim in a US federal court under the US Foreign Sovereign Immunities Act in which the Rezaian family was awarded almost $180 million US dollars in damages.[168]

Iran continues to use espionage offences to detain journalists on political grounds. In 2022, two reporters were charged with conspiring with the intelligence agencies of foreign powers to undermine Iran's national security when they reported the brutal police beating of a 22-year-old protester arrested for failing to cover her hair properly.[169] The death of the protester sparked nationwide unrest.[170] The journalists remain in prison.[171]

[162] WGAD, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Special Rapporteur on the situation of human rights defenders, UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, UN Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, *Letter to the Representative of the Islamic Republic of Iran*, Reference No. IRN 13/2015, 12 August 2015; WGAD, *Rezaian v. Iran* (Opinion no. 44/2015), 3 December 2015, §16; C. Morello, 'Post reporter jailed in Iran faces 4 charges including espionage' (The Washington Post, 20 April 2015). See R. Gladstone & T. Erdbrink, 'Charges Against Jason Rezaian, Washington Post Reporter Held in Iran, Include Espionage' (The New York Times, 20 April 2015).

[163] N. Karimi, 'Closed-door Trial in Iran of Washington Post reporter begins' (The Press Democrat, 26 May 2015); WGAD, *Rezaian v. Iran* Urgent Petition submitted by the Washington Post (21 July 2015), 23–24.

[164] WGAD, *Rezaian v. Iran* (Opinion no. 44/2015), 3 December 2015, §14; US District Court for the District of Columbia, *Rezaian et al v.* Iran Civil Case No. 16-1960, Complaint, 3 October 2016, §88.

[165] US District Court for the District of Columbia, *Rezaian et al v. Iran,* Civil Case No. 16-1960, Complaint, 3 October 2016, §§82, 92.

[166] Ibid.

[167] OHCHR, 'UN human rights experts call on Iran to release journalist Jason Rezaian as he awaits verdict' (14 August 2015); WGAD, *Rezaian v. Iran* (Opinion no. 44/2015), 3 December 2015.

[168] US District Court for the District of Columbia, *Rezaian v. Iran,* Civil Case No. 16-1960, Memorandum Opinion, 21 November 2019. Iran failed to respond to the lawsuit, and Rezaian's US lawyers have noted that Iran is unlikely to pay the judgment voluntarily: 'WilmerHale Wins $180 Million Judgment Against Iran for Jason Rezaian and Family' (WilmerHale, 12 December 2019).

[169] See J. Rezaian, 'Niloofar Hamedi and Elaheh Mohammadi' (Time, 13 April 2023).

[170] A. Kohli, 'What to Know About the Iranian Protests Over Mahsa Amini's Death' (Time, 24 September 2022).

[171] See A. Pourahmadi, 'Hundreds of Iranian journalists call for the release of two colleagues jailed in Evin prison' (CNN, 31 October 2022). CPJ, 'Iranian journalists Niloofar Hamedi and Elahe Mohammadi sentenced' (22 October 2023).

2.4. North and South America

2.4.1. United States: Pentagon Papers

Prior to 2009, only a handful of cases had been brought by the US government against public servants for disclosing confidential information to the media in violation of the Espionage Act.[172] The first, and most famous, concerned The New York Times' publication of portions of the Pentagon Papers, a 7,000-page top secret report commissioned by the Nixon Administration detailing the United States' involvement in Vietnam.[173] Daniel Ellsberg, one of the government contractors involved in the Papers' preparation, transferred the report to New York Times reporter Neil Sheehan. Ellsberg and a colleague who had helped photocopy the Papers were charged with conspiracy, misappropriation of government property and violations of the Espionage Act.[174] The case was ultimately dismissed on the basis of government misconduct after the court found that Ellsberg's phone had been unlawfully tapped and his psychiatrist's office had been broken into by government agents.[175] And the US Supreme Court rejected a parallel application by the US Government to enjoin The New York Times as well as The Washington Post from publishing the full report's contents and findings in the case of *New York Times v. United States,* a decision that has long been heralded as a victory for the free press.[176] While the government argued that publication would 'result in irreparable injury to the national defense',[177] this argument 'fared poorly in court because the most recent of the documents was three years old and because much of the information about which the Government was upset either had no military significance or was already in the public domain, having been revealed at Congressional hearings or published in newspapers'.[178]

Although Justice Blackmun warned in his dissent that if publication results in 'the death of soldiers, the destruction of alliances, the greatly increased difficulty of negotiation with our enemies, the inability of our diplomats to negotiate… prolongation of the war and … further delay in the freeing of United States prisoners, then the Nation's people will know where the responsibility for these sad consequences rests',[179] it appears

[172] See s. I. (Introduction).

[173] US Supreme Court, *New York Times Co. v. United States* 403 U.S. 713, 30 June 1971, Dissenting Opinion of Burger J., 749 n. 6.

[174] N. Chokshi, 'Behind the Race to Publish the Top-Secret Pentagon Papers' (The New York Times, 20 December 2017); S. V. Roberts, 'Ellsberg Indicted Again in Pentagon Case' (The New York Times, 31 December 1971).

[175] M. Arnold, 'Pentagon Papers Charges Are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails "Improper Government Conduct"' (The New York Times, 11 May 1971). Ellsberg leaked a still-classified study about the Taiwan Strait crisis which he had copied at the same time as the Pentagon Papers but chose not to disclose, which shows that the United States was considering the use of atomic weapons against mainland China if the crisis escalated. Ellsberg, who passed away in 2023, released the study in 2017 and highlighted it amid new tensions between the United States and China regarding Taiwan. Ellsberg also suggested that he could have become a test case to challenge the use of the Espionage Act to 'criminalize classified truth-telling in the public interest': see C. Savage, 'Risk of Nuclear War Over Taiwan in 1958 Said to Be Greater Than Publicly Known' (The New York Times, 22 May 2021).

[176] See US Supreme Court, *New York Times Co. v. United States* 403 U.S. 713, 30 June 1971, Dissenting Opinion of Burger J., 749 n. 6.

[177] F. Abrams, 'The Pentagon Papers a Decade Later' (The New York Times, 7 June 1981).

[178] Ibid.

[179] US Supreme Court, *New York Times v. United States* 403 U.S. 713, 30 June 1971, Dissenting Opinion of Blackmun J., 763.

that '[n]one of the dire consequences of publication foreseen by the Government came to pass'.[180]

Although *New York Times v. United States* represents a victory for press freedom, several Justices of the Supreme Court accepted the premise that journalists could be subjected to criminal charges for publishing government information in violation of the Espionage Act.[181] Justice Black and Justice Douglas, in one of the concurring judgments, disagreed, holding that 'there is… no statute barring the publication by the press of the material which the Times and Post seek to use', because Congress used the word 'communicates' in the relevant law, as opposed to 'publish'.[182] Additionally, the Supreme Court did not definitively resolve that issue of the requisite intent, but two concurring Justices stated that the 'Government need not prove an intent to injure the United States or to benefit a foreign nation, but only willful and knowing conduct'.[183] Nor was the Act declared unconstitutional or reformed since then.

2.4.2. United States: Edward Snowden

In 2013, while working as a consultant for the NSA in Hawaii, whistleblower Edward Snowden downloaded a large but 'still-unknown amount of information' which revealed that the NSA was acquiring, storing and searching the telephone call, text and email data of millions of Americans and individuals around the globe.[184] Snowden travelled to Hong Kong and provided journalists with hundreds of classified documents, leading to the publication of a series of articles in The Guardian and The Washington Post exposing this mass surveillance program. Snowden's leaks also led to revelations about similar programs in nations across the world.[185]

In June 2013 the Obama administration charged Snowden with three counts, for theft of government property, unauthorized communication of national defence information and wilful communication of classified intelligence information to an unauthorized person, the latter two charges falling under the Espionage Act.[186] After the United States revoked Snowden's passport and filed a request for Hong Kong to arrest him, Snowden left Hong Kong and flew to Moscow.[187] He then spent 40 days in the

[180] F. Abrams, 'The Pentagon Papers a Decade Later' (The New York Times, 7 June 1981).

[181] See US Supreme Court, *New York Times v. United States* 403 U.S. 713, 30 June 1971, Concurring Opinion of White J., Stewart J., 733–737. See also Concurring Opinion of Marshall J., 745.

[182] Ibid. Section 793(e) of the US Espionage Act provides that 'whoever having unauthorized possession of, access to, or control over … information relating to the national defense … wilfully communicates, delivers [or] transmits … the same to any person not entitled to receive it'. Although the government argued that 'communicates' is 'broad enough to encompass publication', the Justices noted the eight other sections of the law specifically mention 'publish', and held that 'Congress was capable of and did distinguish between publishing and communication in various sections of the Espionage Act'. Ibid. Concurring Opinion of Douglas J., Black J., 721.

[183] Ibid., Concurring Opinion of White J., Stewart J., 738, n 9.

[184] L. Downie & S. Rafsky, 'The Obama Administration and the Press: Leak investigations and surveillance in post-9/11 America' (CPJ, 10 October 2013).

[185] Amnesty International UK, 'Why Edward Snowden should be pardoned' (5 May 2023).

[186] S. Shane, 'Ex-Contractor Is Charged in Leaks on N.S.A. Surveillance' (The New York Times, 21 June 2013). These charges are punishable by up to 10 years' imprisonment each, exposing Snowden to up to 30 years' imprisonment if convicted. See E. MacAskill, 'Edward Snowden: what would happen if He went home—pardon or prison?' (The Guardian, 4 March 2015).

[187] P. Walker & J. Newell, 'Edward Snowden asks for asylum in Ecuador—as it happened' (The Guardian, 23 June 2013).

Moscow airport, seeking (and being rejected for) asylum from 27 countries, before he was granted temporary asylum in Russia, where he remains today.[188]

Snowden stated that he considered his disclosures different from other whistleblowers, arguing that he 'carefully evaluated every single document I disclosed to ensure that each was legitimately in the public interest', and that he chose to allow reputable journalists to determine which documents should be disclosed to the public.[189] He has indicated that he would return to the United States to face trial if given the opportunity to argue a public interest defence.[190] In 2015 the European Parliament narrowly voted in favour of granting protection to Snowden 'in recognition of his status as whistleblower and international human rights defender' and in 2016 a campaign to push for Snowden's pardon amassed support from key human rights organizations such as Human Rights Watch, Amnesty International and the ACLU.[191] And in September 2020, a US federal court found the 'the government may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act ("FISA") when it collected the telephony metadata of millions of Americans'.[192]

2.4.3. United States: Julian Assange

The case against Ellsberg represents one of the few prosecutions for unauthorized disclosures prior to 2009.[193] From that point the Obama administration commenced an unprecedented number of prosecutions for whistleblowing, including against 10 government employees and contractors prosecuted for leaking classified information, eight of these under the Espionage Act.[194] This trend was continued by the Trump administration, which instigated nine prosecutions, six under the Espionage Act,[195] including the indictment against Julian Assange, the first non-government employee or contractor to be charged under the Act for the act of publishing confidential material.[196]

[188] See, e.g., D. Davies, 'Edward Snowden Speaks Out: "I Haven't and I Won't" Cooperate with Russia' (NPR, 19 September 2019); In October 2020, Snowden was granted permanent residency in Russia: A. Troianovski, 'Edward Snowden, in Russia Since 2013, Is Granted Permanent Residency' (The New York Times, 23 October 2020).

[189] G. Greenwald & others, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations' (The Guardian, 11 June 2013).

[190] J. Grierson, 'Edward Snowden would be willing to return to US for fair trial' (The Guardian, 21 February 2016).

[191] T. McCarthy, 'Edward Snowden praises EU parliament vote against US extradition' (The Guardian, 29 October 2015); American Civil Liberties Union (ACLU), 'High-Profile Campaign Calls on Obama to Pardon Edward Snowden' (14 September 2016). See also S. Coliver, 'Why Snowden Won't Get the Public Interest Defense He Deserves' (Open Society Justice, 24 June 2015); D. Ellsberg, 'Daniel Ellsberg: Snowden would not get a fair trial—and Kerry is wrong' (The Guardian, 30 May 2014).

[192] US Court of Appeals, Ninth Circuit, *United States v. Moalin* 973 F.3d 977, 2 September 2020, 7.

[193] See, e.g., US Supreme Court, *New York Times Company v. United States* 403 U.S. 713, 30 June 1971. See also US Court of Appeals, Fourth Circuit, *United States v. Morison* 844 F.2d 1057, 1 April 1988, affirming the 1985 District Court conviction of naval intelligence officer Samuel Morison, for allegedly selling secret photos of a Soviet naval base to the British publication *Jane's Defence Weekly*. He was sentenced under Sections 793(d) and (e) of the US Espionage Act and for theft of government property, and sentenced to two years' imprisonment.

[194] G. Rottman, 'On Leak Prosecutions, Obama Takes it to 11. (Or Should We Say 526?)' (ACLU, 14 October 2014). The two other cases were treated as misdemeanours: see S. Ackerman & E. Pilkington, 'Obama's war on whistleblowers leaves administration insiders unscathed' (The Guardian, 16 March 2015).

[195] US Press Freedom Tracker, 'Incident Database: Leak Cases' reporting on cases between 1/20/2017 to 01/20/2021.

[196] See E. Tucker, 'US Charges WikiLeaks founder with publishing classified info' (Associated Press, 24 May 2019).

Despite the tradition of non-enforcement against journalists, section 793(e) of the Espionage Act prohibits the unauthorized *receipt* of national security secrets which on its face might create criminal liability for reporters, either as co-conspirators or for aiding and abetting the individuals who provided the information.[197] Some legal scholars argue, however, consistently with Justice Douglas and Black's concurrence in *New York Times Co v. United States*, that by omitting 'publishing' from section 793(e), Congress intentionally and purposefully excluded section 793(e)'s applicability to the press.[198]

But in 2019 the US Department of Justice indicted WikiLeaks founder Julian Assange for crimes committed under the Espionage Act, including under section 793(e), and sought to have him returned to the United States from the United Kingdom. The indictment related both to Assange allegedly conspiring with Army Intelligence Analyst Chelsea Manning to hack a US Department of Defense computer,[199] as well as WikiLeaks' publishing secret information. Wikileaks published thousands of documents obtained through Manning, including footage of US personnel killing civilians from a helicopter in Iraq, war logs from Afghanistan and Iraq, diplomatic cables and files from Guantánamo Bay which revealed abuses against inmates such as waterboarding and sleep deprivation.[200] However, the indictment alleges that Assange also published materials 'containing the names of individuals, who risked their safety and freedom by providing information to the United States and our allies' and that he 'communicated the documents containing names of those sources to all the world by publishing them on the Internet'.[201]

Before the UK court determining whether Assange should be extradited, counsel for the US Government emphasized that the publishing charges were 'expressly limited to documents which contained the names of human sources',[202] and alleged that hundreds of sources had been put 'at risk', with some relocated and others having 'disappeared', although 'the US cannot prove at this point that their disappearance was the result of being outed by WikiLeaks'.[203] Assange's defence counsel claimed that the prosecution had misrepresented the facts, and that WikiLeaks had worked for months in partnership with professional media organizations to redact the leaked documents but that one of the media partners had published a book containing the leaked password to the unredacted dataset, leading to its access and publication by other parties. The defence also argued that Assange had attempted to mitigate

[197] S. Vladeck, 'The Espionage Act and National Security Whistleblowing after *Garcetti*' (2007–2008) 57 *American University Law Review* 1531, 1536. See also US Espionage Act 1917, 18 U.S.C. §§793–799.

[198] See K. Wimmer & S. Kiehl, 'Prosecution of Journalists under the Espionage Act: Not so Fast' (2017) 33 *Communications Lawyer* 24, 25.

[199] US Department of Justice, 'WikiLeaks Founder Julian Assange Charged in 18-Count Superseding Indictment' (23 May 2019). See also US Department of Justice, 'WikiLeaks Founder Charged in Superseding Indictment' (24 June 2020), broadening 'the scope of the conspiracy surrounding alleged computer intrusions with which Assange was previously charged'.

[200] See C. Savage, 'Soldier Admits Providing Files to WikiLeaks' (The New York Times, 28 February 2013).

[201] US District Court for the Eastern District of Virgina, *United States v. Julian Assange* Crim. Case 1:18-cr-11, Superseding Indictment, 23 May 2019, Counts 15–17.

[202] UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, §123.

[203] Ibid., §20.

any risk to sensitive sources by notifying the White House and State Department that publication outside WikiLeaks' control was potentially forthcoming.[204]

However, the defence did not dispute that after the initial disclosure by third parties unrelated to Wikileaks, Wikileaks did publish a full unredacted version of the 250,000 diplomatic cables, including the names of human sources, which the United States argued was to prevent Wikileaks from being 'scooped' by others.[205] Assange's defence counsel submitted that Wikileaks' disclosure of the names of human sources was protected by article 10 of the European Convention on Human Rights, on the basis that the risk of harm to a small number of sources was 'unintentional, small and unsubstantiated'[206] and should be weighed against the US Government's involvement in 'serious criminal activity' that the disclosures revealed.[207]

Judge Baraitser, sitting in the English magistrates court, found that the US charges against Assange did not violate the right to freedom of expression under English law and the European Convention on Human Rights.[208] She acknowledged the 'inevitable tension' between the 'vital importance of the press in exposing abuses and miscarriages of justice by reporting information they have received' and the 'strong public interest in keeping the security or intelligence service secure', but noted that no public interest defence is available to charges under the UK Official Secrets Act.[209] The court ultimately held that prosecution of the disclosure of informants' names is necessary in a democratic society in the interests of national security.[210] In response to defence submissions that Wikileaks went to 'extraordinary lengths' to publish the material in a responsible manner, and that the harm to informants alleged by the US Government may not have occurred, the court held that these issues were matters to be determined at Assange's trial, rather than extradition proceedings, but did make a number of comments reflecting disapproval of this argument.[211]

Judge Baraitser opined that 'in the modern era, where "dumps" of vast amounts of data onto the internet can be carried out by almost anyone, it is difficult to see how the concept of 'responsible journalism' can sensibly be applied'.[212] The concept could not, according to the Judge, vest in Assange the right to make the decision to sacrifice the safety of individuals in the name of free speech while 'knowing nothing of their

[204] Reporters without Borders, 'UK: Legal arguments during the first week of Julian Assange's extradition hearing highlight lack of US evidence' (28 February 2020).

[205] UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, §391–392.

[206] Ibid., §122.

[207] Ibid., §122.

[208] Ibid., §122, 137.

[209] Ibid., §147. The decision of *R v. Shayler* [2002] UKHL 11 relates to sections 1 and 4 of the UK Official Secrets Act 1989, both sections that apply to Crown servants: UK House of Lords, *R v. Shayler* [2002] UKHL 11, 21 March 2002. However, the Court in *The Government of the United States of America v Julian Paul Assange* appears to have accepted that both these sections and those which apply to all persons do not incorporate a public interest defence: see, e.g., UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, §147: 'Nor is a "public interest" defence available under the OSA 1989; this was made clear by the House of Lords in *Shayler*.'

[210] UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, §137.

[211] Ibid., §§390, 402.

[212] Ibid., §131.

circumstances or the dangers they faced'.[213] The Court also contrasted Assange's conduct to the 'traditional press' since he was a person who chose to disclose information on the internet without being 'bound by a professional code or ethical journalistic duty or practice', and provided examples of the 'careful editorial decisions' made by news outlets in 'stark contrast' to Assange's 'final, indiscriminate disclosure' on 2 September 2011.[214] Ultimately, however, the Judge found that extradition would be oppressive in light of the 'substantial' risk Assange might commit suicide if extradited.[215] Assange's legal counsel later commented that 'while we were successful … in that we achieved the right outcome' before the Court, it was 'unfortunately for all the wrong reasons' because the Judge 'rejected all of the free speech arguments … all of the arguments about the public interest of these disclosures'.[216]

In December 2021 this decision was overturned by the High Court on the basis of assurances made by the United States as to the prison conditions Assange would face during pretrial or post-conviction detention, and assurances that Assange would be eligible for—and the United States would consent to—a transfer to an Australian prison to serve any custodial sentence imposed on him.[217] Assange continues to appeal his decision in British courts and before the European Court of Human Rights.[218]

Journalists and human rights groups have expressed alarm that the indictment against Assange sets a precedent that allows for criminalization of journalistic activities. Marty Baron, then editor of The Washington Post, decried the indictment as 'criminalizing common practices in journalism that have long served the public interest'.[219] First Amendment experts also opined that 'the U.S. indictment of Assange will continue to cast a dark shadow over investigative journalism'.[220] It is understood that the Obama administration did not go after Assange because of the so-called 'New York Times problem': if prosecutors could charge Wikileaks they could also charge the New York Times for the same conduct, an outcome that many would consider an anathema in the United States.[221] Following the indictment, The New York Times in fact confirmed that it 'obtained precisely the same archives of documents from WikiLeaks, without authorization from the government—the act that most of the charges addressed'. The

[213] Ibid., §131.
[214] Ibid., §§131–132.
[215] Ibid., §§337, 363.
[216] J. Robinson, 'Julian Assange: Repression, Isolation & Lockdown' (Disruption Network Lab, 6 May 2021), at 7:10 mark.
[217] UK High Court of Justice Queen's Bench Division Administrative Court, *The Government of the United States of America v. Julian Paul Assange* [2021] EWHC 3313 (Admin), 10 December 2021. In January 2022, the High Court ruled that Assange could bring a further appeal to the UK Supreme Court on the narrow issue of the timing of the US' assurances regarding Assange's treatment in prison. But in March 2022 the UK Supreme Court refused to hear the appeal on the basis that Assange's application did not 'raise an arguable point of law'. The case went back for determination by Judge Baraister, before the UK Home Secretary signed the extradition order in June 2022. In June 2023, Assange's appeal was rejected by the High Court and a further appeal was signaled: B. Doherty, 'Julian Assange "dangerously close" to US extradition after losing latest legal appeal' (The Guardian, 8 June 2023).
[218] M. Holden, 'Julian assange appeals to European court over U.S. extradition' (Reuters, 2 December 2022).
[219] L. Grove, 'America's Top Newspaper Editors Alarmed by Assange Indictment' (The Daily Beast, 25 May 2019).
[220] Knight First Amendment Institute at Columbia University, 'Knight Institute Comments on Decision to Reject U.S. Request for Extradition of Julian Assange' (4 January 2021).
[221] S. Horwitz, 'Julian Assange unlikely to face U.S. charges over publishing classified documents' (The Washington Post, 25 November 2013).

New York Times also noted that although it 'did take steps to withhold the names of informants in the subset of the files it published', 'it is not clear how that is legally different from publishing other classified information'.[222] An example of a common journalistic practice that the Assange indictment has the potential to criminalize is the use by journalists of secure cloud drop boxes, which allow sources to submit unsolicited material. The use of a SecureDrop box was allegedly pioneered by Wikileaks and is referenced a number of times in the Assange indictment,[223] a process that is now 'a feature' of '21st century journalism'.[224]

One of the reasons that a prosecution against Assange would be so significant is that it would establish a new precedent involving the publication of unlawfully acquired information. The leading First Amendment cases which protect journalists and publishers involve individuals who have obtained information lawfully, whereas even receipt or possession of defence information is criminalized by the Espionage Act.[225] One such case is *Smith v. Daily Mail,*[226] in which the Supreme Court invalidated a West Virginian statute criminalizing the publication of the name of any youth charged as a juvenile offender without approval from the juvenile court. There, the Court held that '[i]f the information is lawfully obtained, as it was here, the state may not punish its publication except when necessary to further an interest' of substantial import.[227] The Supreme Court came to the same conclusion in *Bartnicki v. Vopper,*[228] observing that *New York Times v. United States,* 'raised, but did not resolve, the question 'whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well'.[229] This remains an open question that the Assange prosecution—if it takes place—may decide, with far-reaching consequences.

III. International Legal Standards

As there has been an uptick in espionage and official secrets laws being used against journalists and whistleblowers across the globe, international and regional standards on the free speech implications of this behaviour have developed considerably in recent years. The European Court of Human Rights has amassed a significant body of jurisprudence, including the seminal case of *Bucur and Toma v. Romania*, involving a whistleblower who uncovered unlawful wiretapping by authorities in Romania a few

[222] C. Savage, 'Assange Indicted Under Espionage Act, Raising First Amendment Issues' (The New York Times, 23 May 2019); 'Piecing Together the Reports, and Deciding What to Publish' (The New York Times, 25 July 2010).
[223] US District Court for the Eastern District of Virgina, *United States v. Julian Assange* Crim. No. 1:18-cr-111 (CMH), Second Superseding Indictment, 24 June 2020, §§17, 25.
[224] See UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, Consolidated Annex, §63 (summarizing witness testimony of Professor Michael Tigar).
[225] 18 U.S.C. §§793(c) and (e).
[226] US Supreme Court, *Smith v. Daily Mail Pub. Co.* 443 U.S. 97, 26 June 1979.
[227] Ibid., 104.
[228] US Supreme Court, *Bartnicki v. Vopper,* 532 U.S. 516, 21 May 2001.
[229] Ibid., 528.

months before Edward Snowden's revelations came to light in 2013. Although other bodies have more limited jurisprudence, soft law instruments such as the Tshwane Principles also provide 'highly persuasive' guidance on the international standards that are applicable to secrecy laws.[230] In addition, the wider body of jurisprudence governing the interplay between speech and national security can be applied to the use of espionage and official secrets laws to stifle speech.

1. International Standards Related to Speech Affecting National Security

The 'protection of national security' is one of the legitimate purposes for which speech can be restricted under article 19(3) of the ICCPR,[231] as well as the European Convention and American Convention.[232] Although article 9 of the African Charter on Human and Peoples' Rights does not specify legitimate aims for curtailing 'the right to express and disseminate … opinions within the law', this provision has been consistently interpreted as incorporating the aim of protecting national security, in line with other international treaty standards.[233] 'Security' or 'national security' considerations may also limit the scope of other human rights.[234]

But as the Human Rights Committee has made clear, the restrictions a state imposes on freedom of expression cannot 'put in jeopardy the right itself' and 'the relation between right and restriction and between norm and exception must not be reversed'.[235] As with all restrictions under article 19 of the ICCPR, restrictions for the legitimate purpose of national security must be 'provided by law', pursue a legitimate aim and conform to the strict tests of necessity and proportionality.[236] The burden lies with the state to demonstrate the legal basis for any restrictions to speech.[237] And restrictions must not only comply with the requirements of article 19(3), but must themselves be 'compatible with the provisions, aims and objectives of the Covenant'.[238]

[230] Open Society Justice Initiative, 'Understanding the Tshwane Principles' (12 June 2013). Sometimes the abuses of freedom of expression are so flagrant that courts are not required to examine the nuances and limits of this jurisprudence. See, e.g., WGAD, *Piskorski v. Poland* (Opinion no. 18/2018), 20 April 2018; WGAD, *61 individuals v. United Arab Emirates* (Opinion no. 60/2013), 22 November 2013.

[231] ICCPR Art. 19(3). See ch. 1 (Introduction), s. II.1.2.1.1. (ICCPR: Article 19).

[232] ECHR Art. 10(2); ACHR Art. 13(2)(b).

[233] See ch. 1 (Introduction), s. II.1.2.2.3. (African Charter). ACmHPR, *Good v. Botswana* (Comm. no. 313/2005), 26 May 2010, §§188–189. The ASEAN Human Rights Declaration provides as a general principle that human rights shall be subject to limitations determined by law 'to meet the just requirements of national security' among other purposes: ASEAN Human Rights Declaration Art. 8.

[234] The protection of national security is a legitimate purpose by which six rights under the ICCPR can be limited: Art. 12 (free movement), Art. 13 (procedures applicable to aliens' expulsion), Art. 14 (fair trial), Art. 19 (speech), Art. 21 (assembly) and Art. 22 (association). See also ACHR Arts. 27(1), 32(2); American Declaration Art. XXVIII.

[235] HRC, General Comment No. 34 (2011), §21.

[236] Ibid., §22; see, e.g., ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §101; IACtHR, *Usón Ramírez v. Venezuela* (Series C, no. 207), 20 November 2009, §49.

[237] See HRC, General Comment No. 34 (2011), §27; WGAD, *Chhin v. Cambodia* (Opinion no. 3/2019), 24 April 2019, §48.

[238] HRC, General Comment No. 34 (2011), §26.

The Human Rights Committee has cautioned that 'extreme care must be taken' by states to ensure that treason laws, and 'similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise' are crafted and applied in conformity with the 'strict requirements' of article 19(3).[239] For example, the Committee has held that it is not permissible to 'invoke such laws to suppress or withhold from the public information in the legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders or others, for having disseminated such information'.[240] Although this statement is somewhat circular since it relates only to information that 'does not harm national security', the prohibition on criminal prosecution for publishing such information is clear.

A state's assertion that national security interests are at stake will be given considerable deference by international bodies.[241] The European Court has noted that 'the judgment by the national authorities in a case involving national security is one which [the Court] is not well equipped to challenge'.[242] The Court considered that 'significant weight must' therefore 'attach to the judgment of the domestic authorities, and especially of the national courts, who are better placed to assess the evidence relating to the existence of a national security threat'.[243] The Court found that it 'seldom challenges the legitimate national security aim adduced by the state'.[244]

However, international bodies will not simply accept a state's bald assertion that national security is implicated without reaching their own view.[245] According to the Human Rights Committee, a state must 'demonstrate in a specific and individualized fashion the precise nature of the threat' and 'a direct and immediate connection between the expression and the threat'.[246] For example in a case before the Human Rights Committee, a newspaper editor was convicted for publishing classified reports by security services revealing misconduct within the service.[247] The editor argued that the files did not contain 'any information disclosing forces, means and methods of investigation of criminal cases affecting security interests' of Kazakhstan, but 'merely disclosed possible misconduct by members of the security services . . . and such information by no

[239] Ibid., §30.

[240] Ibid. General Comment No. 34 also notes that it is generally not appropriate to restrict information relating to the commercial sector, banking, or scientific progress under national security laws.

[241] See, e.g., ECtHR (GC), *Janowiec v. Russia* (App. nos. 55508/07 & 29520/09), 21 October 2013, §213.

[242] Ibid. See also ECtHR, *Yam v. United Kingdom* (App. no. 31295/11), 16 January 2020, §§56, 58 (noting that in cases where there are legitimate reasons for the European Court not to 'have sight of the national security material on which decisions restricting' public trials are based, it will 'scrutinise the national decision-making procedure to ensure that it incorporated adequate safeguards to protect the interests' of defendants).

[243] ECtHR, *Liu v. Russia (No. 2)* (App. no. 29157/09), 26 July 2011, §85.

[244] ECtHR Research Division, National security and European case-law (2013), §46.

[245] See, e.g., WGAD, *Xiyue Wang v. Iran* (Opinion no. 52/2018), 23 August 2018, §75 (holding that the government 'did not establish a clear connection between this activity and contemporary national security interests protected under article 19(3)'); ACmHPR, *Media Rights Agenda v. Nigeria* (Comm. no. 224/98), 23 October–6 November 2000, §53 (stating that there must be more than an 'omnibus statement' from the state authorities claiming a security threat).

[246] HRC, General Comment No. 34 (2011), §35 (citing HRC, *Shin v. Republic of Korea* (Comm. no. 926/2000), 16 March 2004, §35).

[247] HRC, *Esergepov v. Kazakhstan* (Comm. no. 2129/2012), 29 March 2016.

means implicates the national security of the State'.[248] The Committee also considered the case of a professional artist who painted and distributed a political artwork entitled 'Rice Planting', and was convicted under the Republic of Korea's National Security Law for 'enemy-benefiting expression'.[249] The Committee held that Korea must demonstrate 'in specific fashion the precise nature of the threat' caused by the author's conduct 'as well as why seizure of the painting and the author's conviction were necessary'.[250] In the absence of this 'individualized justification', the Committee found a violation of article 19(2) and ordered compensation, an annulment of the artist's conviction, legal costs and the painting to be returned in original condition.[251] And where a member of a US youth organization which discussed peace issues between North and South Korea was convicted under the same National Security Law as being a member of an 'enemy-benefiting organization', the Committee held that, even though South Korea had invoked national security concerns by reference to the 'general situation in the country and the threat posed by "North Korean communists"', it had failed to specify the 'precise nature of the threat' the expression posed.[252] As a result, the Committee found the author's conviction was not necessary for the protection of a legitimate aim under article 19(3) and that South Korea should provide compensation and ensure that similar violations do not take place.[253]

The UN Working Group on Arbitrary Detention has required a similar clear and causal link between the restricted expression and the alleged endangerment of national security. In a case in which two Rwandan journalists were charged with crimes against national security for publishing articles that alleged government corruption and criticized the Rwandan authorities, the Working Group held that restrictions under article 19(3) 'must not be overbroad' and that the expression in question did not pose 'any actual, imminent or hypothetical threat to national security'.[254] The Working Group noted that statements such as 'Rwandans have spent 15 years in a coma', 'the war between Kagame's regime and the population' and 'Kagame in difficult times' could not be regarded as 'establishing a sufficient causal link to endangering national security'.[255]

The Working Group has, in some instances, also required states to show a nexus between the expression that has been restricted on the basis of national security and a call for violence.[256] For example, the Working Group found that a women's rights activist in Kurdistan had her freedom of expression violated under the ICCPR when she was

[248] Ibid., §3.8.
[249] HRC, *Shin v. Republic of Korea* (Comm. no. 926/2000), 16 March 2004, §§2.1, 2.2.
[250] Ibid., see also §7.3.
[251] Ibid., §§7.3–7.8. Korean authorities did not return the artwork to the artist and kept it in storage for 29 years, where it suffered some damage. In 2018, the Ministry of Justice decided to transfer the painting to the National Museum of Contemporary Art: see H. Hwang, 'Controversy over anti-state propaganda painting' (The Dong-a-Ilbo, 30 December 2017); 'Controversial painting "Rice Planting" unveiled to public for first time since 1989' (Hankyoreh, 30 January 2018).
[252] HRC, *Park v. Republic of Korea* (Comm. no. 628/1995), 20 October 1998, §§2.2, 2.3, 10.3.
[253] Ibid., §10.3, §12.
[254] WGAD, *Agnès Uwimana Nkusi & Saïdati Mukakibibi v. Rwanda* (Opinion No. 25/2012), 29 August 2012, §57.
[255] Ibid.
[256] See J. Genser, *The Working Group on Arbitrary Detention: Commentary and Guide to Practice* (CUP 2019), 208. See ch. 6 (Terrorism Laws), s. III.3.1 (Harm).

convicted of crimes against the Iranian state for allegedly being a member of a political opposition group, even though she was working within the non-militant wing of that group. The Working Group held that 'the Government did not provide any information … that Ms. Jalalian [was] involved in violent activities … and there were no legitimate grounds to restrict the exercise of her freedoms'.[257] In contrast, the Working Group considered the conviction and detention of a political figure in Bhutan to be lawful in circumstances where he had 'sowed communal discord' between ethnic communities within Bhutan and had 'conspired with others to achieve his ends by violent [as well as] non-violent means'.[258]

Similarly, the European Court has emphasized that the concepts of 'national security' and 'public order' need to be applied with restraint and when 'necessary to suppress release of the information for the purposes of protecting national security and public safety'.[259] And 'even where national security is at stake', the European Court has held that 'measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision'.[260] This requires domestic courts to have access to the classified information needed to effectively assess whether national security interests are enlivened.[261]

In one of the few cases decided by the Inter-American Court of Human Rights touching on speech and national security, *Palamara-Iribarne v. Chile,* the Court ultimately relied on witness testimony that the expression in question did not contain either secret material or information relevant to national security.[262] In this case, Mr. Palamara-Iribarne was convicted for breach of military duties after he attempted to publish a book titled '*Ética y Servicios de Inteligencia*' ('Ethics and Intelligence Services') in which he addressed issues related to military intelligence and the need to ensure compliance with ethical standards. When the author sought the necessary authorization to publish this book, it was denied on the basis that the book threatened 'national security and defence'. However, the Court accepted expert evidence that the book did 'not breach the secrecy and security of the Chilean Navy', but rather contained information obtained from open sources and was written on the basis of Mr. Palamara-Iribarne's training as an intelligence specialist. The Court considered that it was 'logical' that Mr. Palamara-Iribarne's training and military experience helped him to write the book, and to interpret this as entailing an abuse of his freedom of expression 'would prevent individuals from using their education or professional training to enrich the expression of their ideas and opinions'.[263]

[257] WGAD, *Zeinab Jalalian v. Iran* (Opinion no. 1/2016), 18 April 2016, §35. See also WGAD, *Moti Biyya v. Ethiopia* (Opinion no. 18/1999), 15 September 1999, §10.
[258] WGAD, *Tek Nath Rizal v. Bhutan* (Opinion no. 48/1994), 1 December 1994, §18.
[259] ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §54. See also ECtHR, *Görmüş and Others v. Turkey* (App. no. 49085/07), 19 January 2016, §37 (where the Court was 'not convinced' that a search and seizure of a magazine's officers were for the purposes of national security in circumstances where the authorities had not 'instituted criminal proceedings … for activities threatening national security).
[260] ECtHR (GC), *Janowiec v. Russia* (App. nos 55508/07 & 29520/09), 21 October 2013, §213.
[261] Ibid. (in the case of an alleged violation of fair trial rights).
[262] IACtHR, *Palamara-Iribarne v. Chile* (Series C, No. 135), 22 November 2005, §75.
[263] Ibid., §§75–76.

The African Commission addressed an ostensible reliance on national security to restrict expression in a case concerning an Australian academic who was deported by Botswana for an article titled 'Presidential Succession in Botswana: No Model for Africa', in which he criticized the government. The Commission found that such expression was 'purely academic work which criticizes the political system' and that 'there is nothing in the article that has the potential to cause instability, unrest or any kind of violence in the country'.[264] Consequently, the Commission held 'the article posed no national security threat' and Botswana's actions were unnecessary and disproportionate.[265]

Despite this growing body of national security-related jurisprudence, advocates in this area have argued that international treaties and case law provide insufficient guidance on what constitutes national security for the purpose of restricting information, or on how the competing interests should be weighed.[266] Soft law guidance has sought to bolster existing jurisprudence on these issues.

A helpful starting point is the Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights,[267] which relate to exceptions to human rights obligations in general and provide that national security may be invoked only when measures are being taken 'to protect the existence of the nation or its territorial integrity or political independence against force or threat of force', as opposed to 'merely local or relatively isolated threats to law and order'.[268] The Principles provide that national security concerns cannot be used as a pretext for imposing 'vague or arbitrary limitations', and may only be invoked 'when there exist adequate safeguards and effective remedies against abuse'.[269] Finally, countries must not invoke national security to justify measures 'aimed at suppressing opposition' to human rights violations, or to perpetuate repressive practices.[270]

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information[271] were developed in the mid-1990s by a group of experts, and have since been cited as authoritative by a number of international and regional human

[264] ACmHPR, *Good v. Botswana* (Comm. no. 313/2005), 26 May 2010, §199.
[265] Ibid., §199–200.
[266] S. Coliver, 'The Tshwane Principles on National Security and the Right to Information: Their Origins, Contribution to Norm Development, and Impact' (Open Society Justice Initiative, February 2017); see also M. O'Flaherty, 'Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No 34' (2012) 12(4) *Human Rights Law Review* 627, 652: 'With regard to the other grounds for the restriction of freedom of expression (respect for the rights and reputation of others, protection of national security, public order and public health), the Committee declined to elaborate definitions [in General Comment No. 34] … Committee members were understandably reluctant to erect strict definitions that might hamper legitimate future application of Article 19, paragraph 3. Nevertheless, in the view of the present writer the Committee may thus have missed an opportunity to impede abusive invocation by States of the various grounds'.
[267] International Commission of Jurists, 'Siracusa Principles' (1 July 1984).
[268] Siracusa Principles, §§29–30.
[269] Ibid., §31.
[270] Ibid., §32.
[271] Johannesburg Principles. See also UN Special Rapporteur, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur, Joint Declaration on Access to Information and Secrecy Legislation (2004).

rights bodies.[272] The Principles are more specific in addressing the interplay between speech and national security concerns.[273] They clarify the requisite harm and requirement of secrecy, providing that speech may be sanctioned as a threat to national security only if a government can demonstrate that the expression is intended, and likely to, incite immediate violence and there is a 'direct and immediate connection between the expression and the likelihood or occurrence of such violence'.[274] Further, punishment for disclosure of information on national security grounds is not permissible where 'the disclosure does not actually harm and is not likely to harm a legitimate national security interest'.[275]

Most recently, the Global Principles on National Security and the Right to Information, commonly known as the Tshwane Principles, were issued by 22 civil society organizations and academic centres in June 2013.[276] The Tshwane Principles were drafted over a period of two years and involved consultation with over 500 civil society actors, government officials and security experts, as well as five UN and regional 'Special Rapporteurs' whose mandates address freedom of expression and human rights.[277] The Tshwane Principles are 'based on international (including regional) and national law, standards and good practice, and the writing of experts' and provide guidance to those drafting or implementing laws related to state's withholding information on national security grounds, or punishing the publication of such information.[278] They have been endorsed by a broad range of actors, including the UN Special Rapporteur of Freedom of Opinion and Expression, the Parliamentary Assembly of the Council of Europe (PACE) and the Organization for Security and Co-operation in Europe (OSCE).[279]

The Principles recommend that 'national security' is precisely defined in national law.[280] They set out what is *not* a legitimate national security interest, namely if the 'real purpose or primary impact is to protect an interest unrelated to national security'

[272] See WGAD, *Karma v. Indonesia* (Opinion no. 48/2011), 2 September 2011, §21; ACmHPR, *Good v. Botswana* (Comm. no. 313/2005), 26 May 2010, §194; UN Special Rapporteur F. La Rue, *Report on the promotion and protection of the right to freedom of opinion and expression* (2011) UN Doc. A/HRC/17/27, §36.

[273] Johannesburg Principles, Preamble.

[274] Johannesburg Principles, Principle 6. See s. III.4.2.2. (Causation). The Principles also provide a non-exhaustive list of expression which 'shall not constitute a threat to national security': Principle 7.

[275] Johannesburg Principles, Principle 15. See s. III.4.2.1. (Type and severity of harm).

[276] Tshwane Principles (12 June 2013).

[277] Coliver (n 266). The five Special Rapporteurs were: Frank LaRue, the UN Special Rapporteur; Ben Emmerson, the UN Special Rapporteur on Counter-Terrorism and Human Rights; Pansy Tlakula, the ACmHPR Special Rapporteur on Freedom of Expression and Access to Information; Catalina Botero, the OAS Special Rapporteur on Freedom of Expression; and Dunja Mijatovic, the OSCE Representative on Freedom of the Media. The Tshwane Principles are said to build on the Johannesburg Principles as the 'international right of access to information was in the early stages of its development' when the earlier Principles were drafted, and therefore only eight of the principles addressed this right in broad terms.

[278] Tshwane Principles, Introduction and Preamble.

[279] See, e.g., UN Special Rapporteur Frank La Rue: 'The Principles are a major contribution to the right of access to information and the right to truth concerning human rights violations, and I believe they should be adopted by the Human Rights Council. All states should reflect these Principles in their interpretations of national security law' (cited in the Tshwane Principles); 'The Assembly supports the Tshwane Principles and calls on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information': Parliamentary Assembly of the COE Resolution 1954 (2013) on national security and access to information, 2 October 2013. See also Open Society Justice Initative, 'New Principles Address the Balance between National Security and the Public's Right to Know' (12 June 2013).

[280] Tshwane Principles, Definitions.

such as the 'protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law or the functioning of public institutions; strengthening or perpetuating a particular political interest, party or ideology; or suppression of lawful protests'.[281] They also provide that governments can only restrict information where the disclosure of the information poses 'a real and identifiable risk of significant harm to a national security interest' and the risk of harm 'must outweigh the overall public interest in disclosure'.[282] It is not enough that a public authority simply asserts a risk of harm—they must provide 'specific, substantive reasons to support its assertion'.[283] And the Principles make clear that journalists and non-public officials 'may not be sanctioned for the receipt, possession or disclosure to the public of classified information' in any circumstances, and for public personnel, the 'law should provide a public interest defence if the public interest in disclosure of the information … outweighs the public interest in non-disclosure'.[284]

2. Legality

International human rights treaties that restrict speech require that such restrictions are 'provided by law'.[285] This means that, at a minimum, state laws must be precisely drafted and not unduly vague.

International bodies have frequently criticized espionage and official secrets laws on the basis that they are impermissibly vague. For example, the Human Rights Committee expressed concern that Japan's legislation contains 'a vague and broad definition of the matters that can be classified as secret and general preconditions for classification'. The Committee insisted that Japan should ensure that categories of classified information are 'narrowly defined' and that any restriction to the right to receive information 'complies with the principles of legality, proportionality and necessity to prevent a specific and identifiable threat to national security'.[286] Similarly, the Working Group has 'consistently found that vague and overly broad provisions that could result in penalties being imposed on individuals who have merely exercised their rights cannot be regarded as being consistent' with the ICCPR or UDHR.[287] For example, the Working Group condemned Cambodia's espionage provision criminalizing the 'act of giving or facilitating easy access by a foreign States or its agents to information … which undermine[s] the national defence'.[288] In finding a contravention of article 19 of the ICCPR, the Working Group observed that the law is 'so vague as to be inconsistent with international human

[281] Ibid., Definitions.
[282] Ibid., Principle 3.
[283] Ibid., Principle 4.
[284] Ibid., Principles 43, 47. See s. III.5.1. (Public interest defence).
[285] See ch. 1 (Introduction), s. II.1.1.1. (Abuses by the state).
[286] HRC, *Concluding Observations: Japan* (2014) UN Doc. CCPR/C/JPN/CO/6. The Committee also noted, with regard to the same Japanese law, that no individual should be punished 'for disseminating information of legitimate public interest that does not harm national security'. See also s. III.5.1. (Public interest defence).
[287] WGAD, *Chhin v. Cambodia* (Opinion no. 3/2019), 24 April 2019, §49.
[288] Ibid., §19.

rights law', because the 'determination of what constitutes an offence under this provision appears to be left entirely to the discretion of the authorities'.[289]

The European Court of Human Rights also requires laws to be precise. A norm cannot be regarded as a 'law' unless it is 'formulated with sufficient precision to enable the person concerned to regulate his or her conduct: he or she needed to be able—if need be with appropriate advice—to foresee, to a degree that was reasonable in the circumstances, the consequences that a given action could entail'.[290] However, 'consequences need not be foreseeable with absolute certainty'.[291] This approach is reflected in a 2007 resolution by the Parliamentary Assembly for the Council of Europe which proposes that 'legislation on official secrecy, including lists of secret items serving as a basis for criminal prosecution must be clear and, above all, public', with any 'secret decrees establishing criminal liability' considered incompatible with the Council of Europe's legal standards.[292]

Similarly, the Inter-American Court has insisted that if states choose to restrict or limit speech under the criminal law, 'it is necessary to use strict and unequivocal terms, clearly restricting any punishable behaviors, giving meaning to the principle of criminal legality'.[293] For example, in the case of military slander, the Court required the law to describe 'clearly and without ambiguities' the damage that illicit behaviour will cause, or how that behaviour might jeopardize military benefits 'so that the exercise of a military punitive power is justified'.[294] Where such a provision did not delimit the elements of criminal behaviour or 'consider the existence of injury', the Inter-American Court found the law 'too vague and ambiguous' to comply with the legality requirements under article 9 of the Convention or the free-speech protections of article 13.[295]

And the African Court on Human and Peoples' Rights has held, consistent with other regional human right bodies, that domestic laws which restrict freedom of expression must be 'sufficiently clear, foreseeable and compatible with the purpose of the Charter and international human rights conventions'.[296]

Soft law instruments provide further detail as to what is entailed by the requirement that restrictions are 'prescribed by law'. Principle 3(a) of the Tshwane Principles states that laws restricting the right to information on national security grounds must

[289] Ibid., §44. The Working Group has similarly criticized article 443 of Cambodia's Criminal Code, which criminalizes 'the act of having a secret agreement with a foreign State or its agents, with a view to fomenting hostilities or acts of aggression against Cambodia' as impermissibly 'vague and imprecise': WGAD, *Sokha v. Cambodia* (Opinion no. 9/2018), 19 April 2018, §44.

[290] ECtHR (GC), *Perinçek v. Switzerland* (App. no. 27510/08), 15 October 2015, §131.

[291] ECtHR (GC), *Satakunnan Markkinapörssi Oy v. Finland* (App. no. 931/13), 27 June 2017, §143.

[292] Parliamentary Assembly of the COE Resolution 1551 on the Fair trial issues in criminal cases concerning espionage or divulging state secrets, 19 April 2007, §10.2.

[293] IACtHR, *Usón Ramírez v. Venezuela* (Series C, No. 207), 20 November 2009, §55.

[294] Ibid. See s. III.4.2. (Harm). Although *Usón Ramírez v. Venezuela* relates to military slander laws, this case may be indicative of the Court's expected reasoning in future state secrets cases.

[295] IACtHR, *Usón Ramírez v. Venezuela* (Series C, No. 207), 20 November 2009, §57. Article 9 of the American Convention provides that '[n]o one shall be convicted of any act or omission that did not constitute a criminal offense, under the applicable law, at the time it was committed'.

[296] ACtHPR, *Umuhoza v. Rwanda* (App. no. 3/2014), 24 November 2017, §136.

be 'accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction'.[297] The Tshwane Principles also require 'adequate safeguards against abuse, including prompt, full and effective judicial scrutiny' of the validity of any restrictions.[298]

3. Legitimacy

The legitimate aim generally cited by states as justification for espionage and official secrets laws is the protection of national security. A state's claim that speech is being restricted for this purpose will warrant some deference from human rights bodies, albeit not by any means of an unlimited nature. States are still required to point to a 'specific and individualized … threat' rather than a general situation of uncertainty.[299]

Another 'legitimate aim' is however articulated in article 10(2) of the European Convention—one that is not replicated in other international or regional human rights treaties—'preventing the disclosure of information received in confidence'.[300] This limitation 'encompasses confidential information disclosed either by a person subject to a duty of confidence or by a third party, and in particular … by a journalist'.[301] The Court applied this exception in a case in which a journalist was convicted and fined for publishing extracts from a 'confidential' diplomatic paper regarding compensation for Holocaust victims out of assets deposited in Swiss bank accounts.[302] The Court concluded that the journalist could not have obtained the documents without a breach of official secrecy by another individual.[303] And it considered that the relevant 'legitimate aim' that the government was advancing was prevention of the 'disclosure of information received in confidence', not the protection of national security.[304] However, the analysis of proportionality proceeded in largely the same manner as in cases in which the protection of 'national security' was the legitimate aim being pursued.[305]

[297] Tshwane Principles, Principle 3(a). This builds on Johannesburg Principles Principle 1.1. See also UN Special Rapporteur, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur, Joint Declaration on Access to Information and Secrecy Legislation (2004). See s. III.4.1. (Secrecy).

[298] Tshwane Principles, Principle 3.

[299] HRC, General Comment No. 34 (2011), §35 (citing HRC, *Shin v. Republic of Korea* (Comm. no. 926/2000), 16 March 2004, §35). See s. III.1. (International Standards Related to Speech Affecting National Security).

[300] ECHR Art. 10(2).

[301] ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §61. Although these principles apply to both members of the public and civil servants, the Court considers that the 'very nature of civil service requires that a civil servant is bound by a duty of loyalty and discretion', and therefore that the 'duty of discretion owed by civil servants will also generally be a strong one' (ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §§70, 71).

[302] ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §§14–19.

[303] Ibid., §17.

[304] Ibid., §§54, 62.

[305] Ibid., §108–162. See also s. III.4. (Necessity).

4. Necessity

The leading cases at the international level setting out the necessity of interference with speech related to disclosures affecting national security come from the European Court. An early case, *Guja v. Moldova,* involved an employee at the prosecutor's office who sent letters to a newspaper alleging corruption by the prosecutor's office, President and members of parliament in Moldova.[306] The employee was dismissed on the basis that the letters contained information that was secret.[307]

Holding that the employee had a 'duty of discretion', the Court considered that the 'disclosure should be made in the first place to the person's superior', and only where 'this is clearly impractical … the information could, as a last resort, be disclosed to the public'.[308] The Court then articulated five factors that must be considered when assessing the proportionality of restrictions to a whistleblower's speech.[309] First, 'particular attention shall be paid to the public interest involved in the disclosed information'.[310] Second, the authenticity of the information disclosed is relevant and persons who choose to disclose information should 'carefully verify, to the extent permitted by the circumstances, that it is accurate and reliable', consistently with the duties and responsibilities attached to the right to freedom of expression.[311] Third, the Court will consider the damage suffered by the public authority as a result of the disclosure, and whether such damage 'outweighed the interest of the public in having the information revealed'.[312] Fourth, the 'motive behind the actions of a reporting employee is another determinant factor', particularly whether the speaker 'acted in good faith and in the belief the information was true, that it was in the public interest to disclose it and that no other, more discreet, means of remedying the wrongdoing' were available.[313] Finally, an analysis of the penalty and its impact on the speaker is required.[314]

In applying these factors, the Court found a violation of article 10, as the employee had acted in good faith, there were no available procedures for him to report irregularities and the disclosed letters dealt with issues of improper conduct by politicians and the government's attitude to police brutality, matters 'so important in a democratic society' that they outweighed the interest in maintaining public confidence in the prosecutor's office.[315]

These principles were later extended to the national security context in *Bucur and Toma v. Romania*, where an employee of Romania's intelligence service noticed

[306] ECtHR (GC), *Guja v. Moldova* (App no. 14277/04), 12 February 2008.
[307] Ibid., §21.
[308] Ibid., §73. The Court held that it 'must take into account whether there was available to the applicant any other effective means of remedying the wrongdoing which he intended to uncover'.
[309] Ibid., §§74–78. See also ECtHR, Guide on Article 10 of the Convention, 31 August 2022, §§411–415.
[310] ECtHR (GC), *Guja v. Moldova* (App no. 14277/04), 12 February 2008 §74.
[311] Ibid., §75.
[312] Ibid., §76.
[313] Ibid., §77.
[314] Ibid., §78.
[315] Ibid., §§90–97.

irregularities suggestive of unlawful telephone tapping and, after being reprimanded by his superiors for raising this, on an MP's advice he announced his findings at a press conference.[316] The employee was convicted of gathering and imparting secret information and given a two-year suspended sentence.[317]

Although the Court considered the legitimate aim of Romania's interference with the employee's speech was to protect national security, rather than the protection of information disclosed in confidence as in *Guja v. Moldova*, it applied the same five factors articulated in *Guja*.[318] The result was that the Court considered the information divulged was 'clearly of public interest', in light of Romanian society experiencing close surveillance as a former communist regime, the 'extensive media coverage' that followed the press conference, and the fact that interest in publishing the information was 'so important in a democratic society that it outweighs the interest in maintaining public confidence' in the security services.[319] The Court also accepted the good faith of the employee, the fact that he had 'reasonable grounds to believe that the information disclosed was true' and that the penalty was severe and likely to have a 'deterrent effect' on other intelligence officers.[320]

In a 2023 decision concerning disclosure of confidential tax returns by an employee of PricewaterhouseCoopers (PwC) to a journalist, the European Court noted that it was 'fully conscious of the developments which have occurred since the *Guja* judgment was adopted in 2008', particular the 'leading role' that whistleblowers play in democratic societies 'by bringing to light information that is in the public interest'.[321] In this context, the Court decided to 'confirm and consolidate' the *Guja* principles.[322] The Court identified the 'criteria' in the Guja decision as follows:

- 'whether or not alternative channels for the disclosure were available';
- 'the public interest in the disclosed information';
- 'the authenticity of the disclosed information';
- 'the detriment to the employer';
- 'whether the whistle-blower acted in good faith'; and
- 'the severity in of the sanction.'[323]

It then elaborated on each factor. As to the alternative channels for disclosure, the Court recognized that 'certain circumstances may justify the direct use of "external reporting"', such as where the internal reporting channel is 'unreliable or ineffective', the whistle-blower is 'likely to be exposed to retaliation' or the disclosure 'pertains to the

[316] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013.
[317] Ibid., §41.
[318] Ibid., §§84, 93.
[319] Ibid., §101.
[320] Ibid., §§111–113, 115–119.
[321] ECtHR (GC), *Halet v. Luxembourg* (App. no. 21884/18), 14 February 2023, §120. See s. III.5.1 (Public interest defence).
[322] Ibid.
[323] Ibid., §114.

very essence of the activity of the employer'.[324] Regarding the authenticity of the disclosed information, the Court held that a whistle-blower cannot be refused the protection of article 10 'on the sole ground that the information was subsequently shown to be inaccurate' if they have 'diligently taken steps to verify, as far as possible the authenticity' of such information.[325] The Court described the criterion of good faith as a 'determinant factor' in deciding whether a disclosure should be protected, and the Court should accordingly consider whether a whistle-blower was 'motivated by a desire for personal advantage, a 'personal grievance' or 'any other ulterior motive'.[326] On the question of the public interest in disclosures, the Court observed that 'information concerning unlawful acts and practices is undeniably of particularly strong public interest', but that lawful but 'nonetheless reprehensible or controversial' practices may also constitute public interest issues.[327] Similarly, 'a matter that sparks a debate giving rise to controversy' might be in the public interest.[328] Applying these principles, the Court held that the public interest in the information, which 'opened the door to public debate in Europe and Luxembourg on corporate taxation' and 'tax fairness in general',[329] outweighed the detrimental effects to PwC, and accordingly there was no violation of article 10.[330]

4.1. Secrecy

International bodies require that states have an objective basis for designating information as 'secret' or as damaging to national security. The Working Group has found violations of article 19(3) in circumstances where states have failed to provide such reasons.[331] For example, where two individuals were convicted under South Korea's National Security Law, one for allegedly passing information about South Korea's defence budget to a North Korean agent and another for belonging to a pro-reunification group considered to be an 'anti-State organization',[332] the Working Group found that South Korea had not 'specified the secret material in question or the reason for which it was considered to constitute a State secret'.[333] As a result, their convictions violated articles 19 of the ICCPR and UDHR.

Publishing evidence of human rights violations cannot be characterized as a state secret.[334] The Working Group considered China characterizing the names of victims of

[324] Ibid., §122.
[325] Ibid., §126.
[326] Ibid., §128.
[327] Ibid., §141.
[328] Ibid. Four judges in a dissenting opinion held that while they agreed on the need to 'revisit' the *Guja* criteria, the majority's concept of 'public interest', in particular the categories of 'reprehensible while remaining legal' and 'sparking public debate' were 'excessively vague', and that 'anything can fall' into the latter criterion of sparking debate. The dissenting judges also took the view that the domestic courts had remained within the margin of appreciation when balancing the *Guja* criteria: Joint Dissenting Opinion of Judges Ravarani, Mourou-Vikström, Chanturia and Sabato.
[329] Ibid., §185.
[330] Ibid., §202. The Court noted that no long term damage was established by PwC §194.
[331] See, e.g., WGAD, *Abdolfattah Soltani v. Iran* (Opinion no. 26/2006), 1 September 2006, §14; WGAD, *Shi Tao v. China* (Opinion no. 27/2006), 1 September 2006, §19.
[332] WGAD, *Lee Kun-hee v. South Korea* (Opinion no. 29/1994), 29 September 1994, §5.
[333] Ibid., §§5–6. See also WGAD, *Zhao Yan v. China* (Opinion no. 33/2005), 2 September 2005.
[334] WGAD, *Li Hai v. China* (Opinion no. 19/1999) 16 September 1999, §12.

human rights violations as a state secret to be 'contrary to the international procedural standards prescribed in the field of human rights'.[335] Similarly, when a journalist was charged for publishing articles decrying Russia's failure to process radioactive waste material from old nuclear submarines,[336] the Working Group held that 'in no case may information on environmental conditions, emergencies and disasters posing a risk to human life and health be considered a State secret'.[337]

The European Court will find a violation of article 10 if a domestic court accepts that information is classified without examining it on its merits. For example, the Court found a violation of article 10 where a magazine published 'confidential' documents revealing a system of excluding journalists from invitations based on their political leanings, and a military court ordered a search and seizure at the magazine's officers.[338] In circumstances where national courts 'had not verified if the "confidential" classification of the documents in question was justified', the Court held that the interference with expression was not 'necessary'.[339]

Similarly, the European Court has held that information that has become public has lost its confidentiality.[340] In a case concerning the memoirs of a former member of MI5 which included an account of alleged unlawful activities by British security services, the Court considered it 'incontrovertible' that the interference was for the legitimate purpose of the protection of national security; 'likely' that the material was detrimental; and 'improbable' that public interest concerns would outweigh national security implications.[341] However, as the book had already been published in the United States the 'the contents of the book ceased to be a matter of speculation and their confidentiality was destroyed', and in those circumstances restrictions on publication were not necessary in a democratic society.[342]

The Tshwane Principles also provide that if a state wishes to classify a document, classification levels must correspond to the level and likelihood of the harm of disclosure, and that states must provide reasons for classification which 'describe the harm that could result from disclosure, including its level of seriousness and degree of likelihood'.[343] And both the Tshwane and Johannesburg Principles note that once information has been made 'generally available to the public', whether or not by lawful means, a

[335] Ibid., §§9–12.
[336] WGAD, *Grigorii Pasko v. Russian Federation* (Opinion No. 9/1999), 20 May 1999, §§5, 7.
[337] Ibid.
[338] ECtHR, *Görmüş v. Turkey* (App. no. 49085/07), 19 January 2016, §§76–77.
[339] Ibid., §§66, 76–77.
[340] ECtHR, *Observer and Guardian v. United Kingdom* (App. no. 13585/88), 26 November 1991; ECtHR, *Sunday Times v. United Kingdom (No. 2)* (App. no. 13166/87), 26 November 1991.
[341] ECtHR, *Observer and Guardian v. United Kingdom* (App. no. 13585/88), 26 November 1991, §56. See also ECtHR, *Vereniging Weekblad Bluf! v. the Netherlands* (App. no. 16616/90), 9 February 1995, §§40–46 (where a report of the Dutch internal secret service was published and had been widely disseminated and commented on by the media, and therefore 'the protection of the information as a State secret was no longer justified' or necessary in a democratic society).
[342] ECtHR, *Observer and Guardian v. United Kingdom* (App. no. 13585/88), 26 November 1991, §§66, 69–70. Australia's High Court also declined to enforce the UK Attorney General's attempts to seek an injunction to restrain the publication of the memoirs in Australia, on the basis that Australian domestic courts will not enforce the governmental interests of a foreign state: High Court of Australia, *Attorney-General (UK) v. Heinemann Publishers Australia Pty Ltd* ('Spycatcher case') [1988] HCA 25; 165 CLR 30, 2 June 1988.
[343] Tshwane Principles, Principle 11(a)–(c).

state presumptively loses the ability to penalize its publication. The Tshwane Principles state that any effort to stop further publication is presumptively invalid,[344] and the Johannesburg Principles go even further, stating that 'any justification for trying to stop further publication will be overridden by the public's right to know'.[345]

In 2007, the Parliamentary Assembly of the Council of Europe adopted a resolution stating that 'information that is already in the public domain cannot be considered as a state secret, and divulging such information cannot be punished as espionage, even if the person concerned collects, sums up, analyses or comments on such information'.[346] Further, the question of whether the information disclosed is already in the public domain 'should always be a question of fact to be decided by' a judge or jury and 'upon an affirmative answer' the judge 'must in all cases direct an acquittal'.[347]

Similarly, the 2004 Joint Declaration on Access to Information and Secrecy Legislation, an instrument drafted and adopted by a number of UN and regional Special Rapporteurs on free speech, recommends that 'secrecy laws should define national security precisely and indicate clearly the criteria which should be used in determining whether or not information can be declared secret, so as to prevent abuse of the label "secret" for purposes of preventing disclosure of information which is in the public interest'.[348]

4.2. Harm

4.2.1. Type and severity of harm

Under international standards, speech cannot be penalized on national security grounds without establishing harm. The Human Rights Committee requires a state to show the 'specific and individualized … threat' that a restriction to speech is addressing if penalties are to be considered necessary.[349] The Working Group has also found that certain harm must flow from the speech, at least before any criminal penalty can be imposed. In a case where a writer and history teacher was sentenced to 10 years' imprisonment for allegedly seeking to publish separatist content regarding Tibet, including the number and location of Chinese military installations, the Working Group found a violation of article 19 of the ICCPR.[350] The Working Group held that 'even though the

[344] Ibid., Principle 49(b).

[345] Johannesburg Principles, Principle 17.

[346] Parliamentary Assembly of the COE Resolution 1551 on Fair trial issues in criminal cases concerning espionage or divulging state secrets (2007), §10.1. The Resolution was spurred by a number of high-profile espionage cases against journalists, lawyers and scientists in Russia, as well as US, German, Italian and Swiss authorities threatening to prosecute journalists in relation to the CIA's extraordinary rendition program. This Resolution was cited by the European Court in ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §88.

[347] Parliamentary Assembly of the COE Resolution 1551 on Fair trial issues in criminal cases concerning espionage or divulging state secrets (2007), §10.9.

[348] UN Special Rapporteur, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur, Joint Declaration on Access to Information and Secrecy Legislation (2004).

[349] See, e.g., HRC, General Comment No. 34 (2011), §35; HRC, *Esergepov v. Kazakhstan* (Comm. no. 2129/2012), 29 March 2016, §11.9 (finding a violation of article 19 'in the absence of sufficient justification … as to the way publishing the documents in question jeopardized the public order', beyond 'a general reference to the permissible grounds for restrictions under art. 19(3)'). See s. III.1. (International Standards Related to Speech Affecting National Security).

[350] See WGAD, *Dolma Kyab v China* (Opinion no. 36/2007), 30 November 2007, §15.

ideas of the group may be contradicting the official policy of the government, the exercise of the right to freedom of expression and association cannot be punished as such, if there are no violent acts committed on behalf of the group and there is no factual proof of resort to or advocacy of violence'.[351]

The European Court of Human Rights has required a demonstration that the speech is 'capable of causing considerable damage' to national security or a state institution before it can be penalized under national security laws.[352] The Court considered this in a case where an engineer in the air force was sentenced by a Greek military court to a suspended sentence of five months' imprisonment for disclosing military secrets to a private company. The prosecution arose after he prepared a study for that company about a different missile to the one he was designing for the air force, but experts suggested this nonetheless involved 'some transfer of technical knowledge'.[353] The Court took the view that 'disclosure of the State's interest in a given weapon and that of the corresponding technical knowledge, which may give some indication of the state of progress of its manufacture, are capable of causing considerable damage to national security', and consequently that the Greek courts had not overstepped the 'margin of appreciation' left to domestic authorities on national security matters in convicting and sentencing the speaker.[354]

The Court however reached the opposite conclusion—and found that there was no 'considerable damage to national security'—in a case where a journalist was convicted and fined for 'sharing secret information' with colleagues about Romanian military operations in Afghanistan.[355] The Court weighed whether 'the applicant's actions were, at the relevant time, capable of causing "considerable damage" to national security'[356] and concluded that the government had not demonstrated this harm, even though 'secret information concerning military operations in a conflict zone is *a priori* information that must be protected'.[357] This was because the information was outdated and declassified and a Romanian prosecutor had considered that it 'was not likely to endanger national security but would only harm the interests of the Romanian State and its armed forces'.[358] As a result, the measures taken against the journalist 'were not reasonably proportionate to the legitimate aim pursued, in view of the interests of a democratic society in ensuring and maintaining freedom of the press'.[359]

[351] Ibid. See also WGAD, *Chhin v. Cambodia* (Opinion no. 3/2019), 24 April 2019, §46. Cf. WGAD, *Shi Tao v. China* (Opinion no. 27/2006), 1 September 2006, §7 (where the Working Group found a violation of article 19 in circumstances where it was 'not convinced' that a journalist providing overseas publications with the Chinese government's warnings regarding the anniversary of Tianamen Square could 'result in a situation of extreme gravity').

[352] See, e.g., ECtHR, *Hadjianastassiou v. Greece* (App. no. 12945/87), 16 December 1992, §§45–47.

[353] Ibid.

[354] Ibid.

[355] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §89.

[356] Ibid., §89, citing ECtHR, *Hadjianastassiou v. Greece* (App. no. 12945/87), 16 December 1992. The other factors considered by the Court, citing ECtHR (GC) *Stoll v. Switzerland*, were 'the interests at stake, the conduct of the applicant, the review of the measure by the domestic courts and whether the penalty imposed was proportionate': ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §86.

[357] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §89.

[358] Ibid., §§28, 89.

[359] Ibid., §99.

According to the European Court, the question of whether speech causes 'considerable damage' is one of many factors to be balanced in an assessment of necessity. And on a number of occasions the Court has found that the public interest in speech which reveals illegal or questionable activities within state institutions outweighs the damage such speech causes to 'public confidence' in that institution.[360] For example, in the *Bucur* case, the Court found that 'the general interest in the disclosure of information revealing illegal activities within the [Romanian Intelligence Services] was so important in a democratic society that it prevailed over the interest in maintaining public confidence in that institution'.[361]

The European Court adopted similar reasoning in finding a violation of article 10(2) where a military court ordered a search of a magazine's offices after it published 'confidential' documents revealing that the armed forces were excluding certain journalists from invitations based on their political leanings.[362] The Court held that neither the authorities nor the national courts had demonstrated why the article could be the source of 'difficulties of such a nature as to cause "considerable damage" to the interests of the state', and that the public interest in disclosing the armed forces' questionable practices outweighed 'the interest in maintaining public confidence in this institution'.[363]

The European Court's assessment of harm also takes into account how widely the information was disseminated through the speech.[364] When a journalist had only disclosed to his colleagues, and not yet published, copies of secret documents belonging to a Romanian military unit, the European Court considered this limited disclosure as a relevant—but not determinative—factor to be weighed in the overall assessment of necessity.[365] The European Court did not explicitly reject the Romanian courts' finding that the journalist 'had committed an offence by virtue of having shared secret military information with other people'.[366] This was despite third party interveners such as the Open Society Justice Initiative and the International Commission of Jurists pressing the Court to do so, arguing that there was 'growing support in international and national law and practice against sanctions for unauthorized possession, including in the area of national security', citing European countries such as Albania, Moldova and Poland which do not publish unauthorized possession alone, as well as other states which apply sanctions only to public servants.[367] The organizations submitted that 'journalists and

[360] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §115. See ss III.4. (Necessity) and III.5.1. (Public interest defence); ECtHR, *Görmüş v. Turkey* (App. no. 49085/07), 19 January 2016, §63.

[361] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §115.

[362] ECtHR, *Görmüş and others v. Turkey* (App. no. 49085/07), 19 January 2016.

[363] Ibid., §§62–63.

[364] Most cases that come before international human rights bodies relating to espionage and official secrets laws address the publication of secret material. Cases addressing receipt and possession of information do not impact speech directly and are therefore outside the scope of this chapter. There is however international guidance suggesting that espionage or official secrets laws with criminal penalties should only cover public disclosures, as opposed to non-communicative behaviour such as the possession or gathering of information. See, e.g., ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §§68–72.

[365] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §98.

[366] Ibid., §85.

[367] Ibid., §§66–67; ECtHR, *Gîrleanu v. Romania* (App. No. 50376/09), 26 June 2018, Open Society Justice Initiative et. al, Joint Third Party Submission (8 October 2013). See s. II.1.1.3. (Type of disclosure).

other similarly protected persons may be subject to sanctions for possession or disclosure [of information of] public interest … only in exceptional circumstances'.[368] The Court noted that the sanctions were imposed before publication, and therefore 'had the purpose of preventing him from publishing and sharing the secret documents he had in his possession'.[369] And it ultimately found a violation of article 10, holding that the sanctions against the journalist—fees totalling 870 Euros—were disproportionate.[370]

The Inter-American Court has not articulated a detailed harm test for restrictions to speech by way of official secrets laws, but has held that, at a minimum, laws penalizing speech must 'specify the injury required' for conduct to fall within their ambit.[371] The Court considered this requirement in a case in which a former member of the military was sentenced to five years and six months' imprisonment in military criminal court for slandering the armed forces of Venezuela by making comments in a television program regarding the alleged use of a 'flamethrower' as punishment against soldiers.[372] The Court criticized the slander provision as 'limited to foreseeing the sanction, without taking into account the specific injury of causing discredit, damaging the good reputation or prestige, or causing damage to the detriment of the passive subject'.[373] Without the inclusion of a damage requirement, the Court reasoned, this law 'allows that the subjectivity of the offended party determine the existence of crime, even when the active subject did not have the intent to injure, offend, or disparage the passive subject', and it was therefore in violation of the right to freedom of expression in the American Convention.[374]

The Tshwane Principles also specify the need for a state to show harm before penalizing speech on national security grounds. Specifically, there should be a requirement to show 'a real and identifiable risk of causing significant harm' to a legitimate national security interest before prosecuting public officials for leaks of national security information.[375] A public authority must provide 'specific, substantive reasons' to support its assertion that a risk of harm exists, and that risk 'must outweigh the overall public interest in disclosure'.[376] And the 2019 Declaration of Principles of Freedom of Expression and Access to Information in Africa considers that speech cannot be restricted on national security grounds unless 'there is a real risk of harm to a legitimate interest'.[377]

[368] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §67.
[369] Ibid., §98.
[370] Ibid., §99. The Court also considered the journalist's 'conduct', observing that his 'first step after coming into possession of the information in question was to discuss it with the institution concerned by the leak, the Romanian Armed Forces'. And it found that in circumstances where the documents had been declassified, the decision to impose sanctions 'should have been more thoroughly weighed'. See ss III.5.2. (Reasonableness of the publication) and III.6. (Penalties). ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §92–98.
[371] IACtHR, *Usón Ramírez v. Venezuela* (Series C, No. 207), 20 November 2009, §56. Although *Usón Ramírez v. Venezuela* relates to military slander laws, this case may be indicative of the Court's expected reasoning in future state secrets cases.
[372] Ibid., §37.
[373] Ibid., §56.
[374] Ibid., §56 (finding violations of both Arts 9 and 13).
[375] Tshwane Principles, Principle 46(b)(ii).
[376] Tshwane Principles, Principles 3–4. See also Johannesburg Principles, Principles 1.3, 2, 6.
[377] ACmHPR, Declaration on Principles of Freedom of Expression and Access to Information in Africa (2019), Principle 22(5). See s. III.4.2.2. (Causation).

4.2.2. Causation

Limited jurisprudence from international bodies has grappled with the question of whether a state is required to demonstrate a causal link between the speech and the harm to national security, and if so to what standard. The Human Rights Committee stated in General Comment No. 34 that 'when a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate … the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat'.[378] However, there is only limited case law that examines how the 'direct and immediate connection' standard should be applied in practice.[379] The Working Group on Arbitrary Detention has also referenced, but not explained, this standard on a number of occasions.[380] Similarly, although the European and Inter-American Courts have articulated harm requirements[381] they have not set out detailed guidance on how to apply them.[382]

Aside from the requirement that disclosures by public personnel of national security information which do not 'pose a real and identifiable risk of significant harm' are not sanctioned, the Tshwane Principles do not impose a specific causation standard.[383] But the Johannesburg Principles adopt the Human Right Committee's 'direct and immediate' standard, and state that expression may be punished as a threat to national security only if a government can demonstrate that (a) the expression is intended to incite immediate violence; (b) is likely to incite such violence; and (c) there is a *direct and immediate* connection between the expression and the likelihood or occurrence of violence.[384] And the 2019 Declaration of Principles of Freedom of Expression and Access to Information in Africa states that there should be 'a close causal link between the risk of harm and the expression' for states to restrict such expression on national security grounds.[385]

[378] HRC, General Comment No. 34 (2011), §35, citing *Shin v. Republic of Korea* (Comm. no. 926/2000), 16 March 2004.

[379] See ch. 3 (Hate Speech), s. II.1.2. (Harm); Michael O'Flaherty, who served as the Human Rights Committee's rapporteur for the development of General Comment No. 34, has noted that this nexus was not in the original draft of the General Comment and 'sets a high bar for restrictions—it will be of interest to see whether it will be accepted by commentators': O'Flaherty (n 266) 627, 649.

[380] WGAD, *Gulmira Imin v. China* (Opinion no. 29/2012), 29 August 2012, §28; WGAD, *Ziyuan Ren v. China* (Opinion no. 55/2014), 21 November 2014, §28; WGAD, *Zhen Jianghua v. China* (Opinion no. 20/2019), 1 May 2019, §71.

[381] See s. III.4.2. (Harm).

[382] See s. III.4.2.1. (Type and severity of harm). In the context of defamation laws, the European Court has considered whether speech had the 'capacity—direct or indirect—to lead to harmful consequences'. ECtHR, *Alekhina v. Russia* (App. no. 38004/12), 17 July 2018, §220 (emphasis added). See also ECtHR (GC), *Perinçek v. Switzerland* (App. no. 27510/08), 15 October 2015, §207. See ch. 2 (Insulting Speech), s. III.3.2. (Causal link between the speech and the harm). See further IACtHR, *Usón Ramírez v. Venezuela* (Series C, no. 207), 20 November 2009, §55.

[383] Tshwane Principles, Principle 3. However, the Tshwane Principles suggest that when classifying documents, public authorities should provide reasons for classification which describe the harm that could result from disclosure, 'including its level of seriousness and degree of likelihood': Principle 11.

[384] Johannesburg Principles, Principle 6 (emphasis added).

[385] ACmHPR, Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019), Principle 22.

4.3. Intent

The minimum intent that should be required for prosecution or other penalization of the publication of secret government material is not generally addressed in detail by international human rights bodies.[386] But international bodies take motive and intent into account in the context of assessing the *conduct* of a speaker to determine whether there is an applicable 'reasonable publication' or 'responsible journalism' defence for a speaker who was acting in good faith.[387] And the European Court considers the motive of a whistleblowing employee to be a 'determinant factor in deciding whether a particular disclosure should be protected or not'.[388] The Court has held that 'it is important to establish that, in making the disclosure, the individual acted in good faith and in the belief that the information was true, that it was in the public interest to disclose it and that no other, more discreet, means of remedying the wrongdoing was available to him or her'.[389]

5. Exclusions, Exceptions and Defences

5.1. Public interest defence

Although state practice is very mixed, and many leading democracies fail to recognize a 'public interest defence' in their laws,[390] there is consensus among international and regional human rights bodies that the 'public interest' in the content of information is a relevant factor in the determination of whether it is 'necessary' to penalize its publication, and must be weighed against the harm speech may cause.

The Human Rights Committee has stated that it is not permissible to use national security laws 'to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information'.[391]

Similarly the European Court of Human Rights has held that that there is 'little scope' for restrictions on free speech 'in two fields, namely political speech and matters of public interest'.[392] Accordingly, 'a particularly narrow margin of appreciation' will be accorded to states attempting to penalize speech concerning a 'matter of the public interest'.[393] The European Court has held that 'the public interest involved in

[386] Cf. ch. 2 (Insulting Speech), s. III.3.1. (Intent) and ch. 3 (Hate Speech), s. III.2.3.2. (Intent).
[387] See s. III.5.2.3. ('Responsible journalism').
[388] ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §77.
[389] Ibid., §77.
[390] See s. II.1.4.1. (Public interest).
[391] HRC, General Comment No. 34 (2011), §30. General Comment No. 34 also notes that it is generally not appropriate to restrict information relating to the commercial sector, banking, or scientific progress under national security laws.
[392] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §49. See, similarly, ECtHR (GC), *Sürek v. Turkey (No. 2)* (App. no. 24122/94), 8 July 1999, §60, citing *Wingrove v. United Kingdom* (App. No. 17419/90), 25 November 1996, §58.
[393] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §49. For discussion on the 'margin of appreciation' doctrine generally, see ch. 1 (Introduction), s. II. 3 (Jurisprudence). See also ECtHR, Guide on Article 10 of the Convention, 31 August 2022, §488.

the disclosed information' constitutes a factor to be balanced in its proportionality assessment where whistleblowers disclosed information received in confidence.[394] The Court has recognized that public officials may become 'aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest', and therefore the signalling of this illegal conduct or wrongdoing should, 'in certain circumstances, enjoy protection', as 'the interest the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence'.[395] And the Court has held that this may be particularly relevant when analysing speech by a journalist since the press has a 'duty … to impart … information and ideas on all matters of public interest'[396] and 'press freedom assumes even greater importance in circumstances in which State activities and decisions escape democratic or judicial scrutiny on account of their confidential or secret nature'.[397]

The European Court applied these factors in *Stoll v. Switzerland*, finding that the publishing of extracts from a confidential diplomatic paper regarding compensation for Holocaust victims out of assets deposited in Swiss bank accounts was in the public interest as it addressed issues of a 'significant moral dimension which meant that it was of interest even to the wider international community', and considering the impassioned debate in Switzerland about this issue at the time.[398] However, the Court found that the publication was liable to 'cause considerable damage' in Swiss negotiations, that the truncated and reductive article was liable to mislead readers, which detracted from its public interest and finally that the fine imposed was not disproportionate. Consequently, the Court found no violation of article 10.

And in *Bucur and Toma v. Romania,* these principles were applied in a national security context. The Court held that the information—which revealed state-sponsored surveillance of journalists, politicians and businessmen—was 'clearly in the public interest'. The 'extensive media coverage' of the press conference at which the information was revealed was held to 'demonstrate' this public interest.[399] And the Court observed that although the information disclosed related to 'abuses committed by high-ranking officials' and therefore 'affected the democratic foundations' of Romania, the domestic

[394] ECtHR (GC), *Guja v. Moldova* (App no. 14277/04), 12 February 2008, §74. See also §76: A further factor was the damage 'suffered by the public authority as a result of the disclosure in question and … whether such damage outweighed the interest of the public in having the information revealed'. See s. III.4.2. (Harm). The other factors considered by the court where 'the authenticity of the information'; 'the motive behind the actions of the reporting employee'; whether the employee took steps to report the matter internally or whether this was 'impracticable'; and 'the penalty imposed … and its consequences': ECtHR (GC), *Guja v. Moldova* (App no. 14277/04), 12 February 2008, §§74–79, 112, 137. See s. III.4 (Necessity).

[395] ECtHR (GC), *Guja v. Moldova* (App no. 14277/04), 12 February 2008, §§72–74.

[396] ECtHR (GC), *Pentikäinen v. Finland* (App. no. 11882/10), 20 October 2015, §88. See ch. 1 (Introduction), s. II.3.2.5. (Relevance of whether the speaker is a journalist). See also ECtHR (GC), *Von Hannover v. Germany (No. 2)* (App. nos. 40660/08 & 60641/08), 7 February 2012, §102; ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §50.

[397] ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §110.

[398] Ibid., §§115–120.

[399] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §101. See also ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §120 ('there can be no doubting the public interest in the issue … which was the subject of impassionate debate in Switzerland').

courts had not taken the public interest in the information into account.[400] Taking the other factors articulated in *Guja* into account—namely the authenticity of the information disclosed, the good faith of the official and the severity of the sanction—the Court held that the two-year suspended sentence for imparting secret information was disproportionate.

International bodies have not clearly defined the term 'public interest': in particular whether this is an objective test or a description of what the public is *interested in* regardless of its objective worth.[401] However, the European Court has held that 'the definition of what might constitute a subject of public interest will depend on the circumstances of each case' and that 'the public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree … especially in that they affect the well-being of citizens or the life of the community'.[402] The Court has therefore made clear that 'the press's contribution to a debate of public interest cannot be limited merely to current events or pre-existing debates', as the press can also have the role of bringing issues to light.[403]

The European Court has recently provided a more detailed definition of the 'public interest' in a case concerning the disclosure of confidential tax returns to a journalist by an employee of the accounting firm PwC who was later dismissed.[404] The European Court held that that 'information concerning unlawful acts and practices is undeniably of particularly strong public interest', but that lawful but 'nonetheless reprehensible or controversial' tax evasion practices may also constitute public interest issues, as can 'a matter that sparks a debate giving rise to controversy'.[405]

[400] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §103. Although the Court did not address this directly in finding that domestic courts had not considered the public interest, the applicant argued that the documents disclosed could not be classified pursuant to article 24(5) of Romania's law on the protection of classified information, which forbids the classification of any information for the purpose of concealing violations of law: §88.

[401] Cf. UK Law Commission, *Protection of Official Data Report* (2020), §§11.76–11.81, which provides that there should be a public interest defence under the UK Official Secrets Act if a person 'proves, on the balance of probabilities, that: (a) it was in the public interest for the information disclosed to be known by the recipient; and (b) the manner of the disclosure was in the public interest'. However, the Law Commission decided to 'make no further recommendation beyond this in respect of the form of the defence', acknowledging that 'there are various ways such a defence could be drafted'.

[402] ECtHR (GC), *Satakunnan Markkinapörssi Oy v. Finland* (App. no. 931/13), 27 June 2017, §171; ECtHR (GC), *Magyar Helsinki Bizottság v. Hungary* (App. no. 18030/11), 8 November 2016, §162. See ch. 2. (Insulting Speech), s. III.4.2. (Public interest).

[403] ECtHR, *Couderc and Hachette Filipacchi Associés v. France* (App. no. 40454/07), 10 November 2015, §114. See also Baroness Hale of Richmond in UK House of Lords, *Jameel & others v. Wall Street Journal Europe* [2006] UKHL 44, 57: 'there must be a real public interest in communicating and receiving the information. This is, as we all know, very different from saying that it is information which interests the public—the most vapid tittle-tattle about the activities of footballers' wives and girlfriends interests large sections of the public but no-one could claim any real public interest in our being told all about it. It is also different from … whether the information is "newsworthy". That is too subjective a test, based on the target audience, inclinations and interests of the particular publication. There must be some real public interest in having this information in the public domain'. See ch. 2 (Insulting Speech), ss IV.3, 9, 12, 14 (Recommendations).

[404] ECtHR (GC), *Halet v. Luxembourg* (App. no. 21884/18), 14 February 2023, §120. See s. III.4 (Necessity) (discussing *Halet v. Luxembourg*).

[405] Ibid., §141. However, four judges of the Court argued that the latter two categories were 'excessively vague', and in particular that 'anything can fall' within the category of a matter which 'sparks a debate giving rise to a controversy': see Ibid., Joint Dissenting Opinion of Judges Ravarani, Mourou-Vikström, Chanturia and Sabato.

The Inter-American Court of Human Rights similarly considers the public interest to be a relevant factor in determining the necessity of any restriction on speech. The Court considers it 'logical and appropriate that statements concerning public officials and other individuals who perform public services are afforded … greater protection, thus allowing some latitude for broad debate, which is essential for the functioning of a truly democratic system'.[406] The Court applied this reasoning to speech regarding the conduct of a Naval prosecutor in military proceedings in Chile, holding that using criminal contempt laws was a disproportionate response to 'criticism leveled at government institutions and their members, thus suppressing debate' and restricting freedom of expression.[407] More recently, the OAS Special Rapporteur confirmed that 'under no circumstances journalists, members of the media, or members of civil society who have access to and distribute classified information they consider to be in the public interest may be subjected to subsequent punishment'.[408]

International experts have called for public interest to be clearly defined as a defence to any charge under espionage and official secrets laws.[409] According to the Tshwane Principles, non-public officials should receive a total exemption from liability, and cannot be sanctioned for the receipt, possession or disclosure to the public of classified information that is in the public interest in any circumstances.[410] When a disclosure is made by a state official, the Tshwane Principles advocate for a three-part test.

First, certain categories of wrongdoing should be considered a 'protected disclosure', regardless of the classification of the information, namely: criminal offences; human rights or humanitarian law violations; corruption; damage to public health and safety; danger to the environment; abuse of public office; miscarriages of justice; mismanagement or waste of resources and retaliation for disclosure or deliberate concealment of any of the categories.[411] Secondly, public personnel who make disclosures should be protected if the person had reasonable grounds to believe the disclosure tended to show one of the protected categories of wrongdoing.[412] Thirdly, the Principles outline the manner in which public personnel must first disclose internally or to an independent oversight body, and when it is reasonable not to have done so.[413] The Tshwane Principles also include a proportionality component, requiring that the person making the disclosure only disclosed the information that was reasonably necessary to bring to light

[406] IACtHR, *Palamara-Iribarne v. Chile* (Series C, No. 135), 22 November 2005, §82.
[407] Ibid., §88.
[408] OAS Special Rapporteur, *Derecho a la información y seguridad national* (2020), § 185 (citing UN Special Rapporteur and OAS Special Rapporteur, Joint declaration on surveillance programs and their impact on the freedom of expression (2013)).
[409] See also, e.g., UK Law Commission, *Protection of Official Data Report* (2020).
[410] Tshwane Principles, Principle 47. Principle 47(b) also provides that persons cannot be charged with conspiracy or other crimes for having 'sought and obtained' classified information. However, the Principles are 'not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information'. Principle 48 provides for the protection of the confidential sources of non-public personnel.
[411] Ibid., Principle 37.
[412] Ibid., Principle 38. Motivation for disclosure is irrelevant except where a disclosure is proven to be knowingly untrue.
[413] See s. III.5.2. (Reasonableness of the publication).

the wrongdoing.[414] If these conditions are fulfilled, the Tshwane Principles hold that a whistleblower should not be subjected to criminal or civil liability or other forms of retaliation.[415] The Tshwane Principles also provide a 'catchall' provision recommending that even if a disclosure does not fall within a specifically protected category, public personnel should nonetheless be protected from prosecution for disclosures where the public interest in the disclosure of the information outweighs the public interest in its non-disclosure.[416]

The Johannesburg Principles provide for a similar, albeit less detailed, balancing framework centred on the idea that no person should be punished for disclosure of information if the disclosure does not or is not likely to harm a legitimate national security interest, or the public interest in knowing the information outweighs the harm in disclosure, and establishing a category of 'protected information' including 'information communicating alleged violations of human rights and humanitarian law'.[417] The 2004 Joint Declaration on Access to Information and on Secrecy Legislation issued by UN and regional Special Rapporteurs on freedom of expression, Parliamentary Assembly of the Council of Europe and the OSCR also advocate for states to amend secrecy legislation to accommodate a public interest defence.[418]

5.2. Reasonableness of the publication

The European Court and the Tshwane Principles suggest that the conduct of the speaker may be relevant to a determination of whether their speech can be penalized.[419] This relates to the manner in which the material was obtained, steps taken to verify the material, and efforts to report the wrongdoing it exposes using internal channels.

5.2.1. Manner of obtaining the information and steps to verify it

According to the European Court, 'freedom of expression carries with it duties and responsibilities and any person who chooses to disclose information must carefully verify, to the extent permitted by the circumstances, that it is accurate and reliable'.[420]

[414] Tshwane Principles, Principle 40(b).

[415] Ibid., Principle 41. And these rights and remedies cannot be waived or limited by an agreement or condition of employment: Principle 41(e).

[416] Ibid., Principle 43. A list of factors is provided as relevant considerations in this balancing exercise: whether the extent of the disclosure was reasonably necessary; the extent and risk of harm to the public interest caused by the disclosure; whether the whistleblower had reasonable grounds to believe the disclosure was in the public interest; whether they attempted to make the disclosure through the internal or independent procedures and the existence of exigent circumstances justifying the disclosure.

[417] Johannesburg Principles, Principle 7. The category of 'protected expression', the 'peaceful exercise of which shall not be considered a threat to national security' includes but 'is not limited to': advocacy of non-violent change of government, criticism or insult to the nation, government and its agents, objection on the grounds of religion, belief or conscience and information communicating alleged violations of human rights and humanitarian law.

[418] UN Special Rapporteur, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur, Joint Declaration on Access to Information and Secrecy Legislation (2004). See also Parliamentary Assembly of the COE Resolution 1729(2010) on Protection of 'whistle-blowers', 29 April 2010; CoM Recommendation CM/Res (2014)7 of the Committee of Ministers to member States on the protection of whistleblowers, 30 April 2014; OSCE, 'Access to information by the media in the OSCE region: trends and recommendations' (2 May 2007); ACmHR, Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), Principle 35.

[419] See ss III.4.3. (Intent) and III.5.1. (Public interest defence).

[420] ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §75.

The Court also considers whether the speaker has 'acted in good faith and in the belief that the information was true',[421] and whether 'the manner in which a person obtains information considered to be confidential or secret may be of some relevance for the balancing of interests to be carried out in the context of article 10 §2'.[422]

The Court applied these principles in a case in which a journalist was convicted and fined for 'sharing secret information' with colleagues concerning Romanian military operations in Afghanistan.[423] The Court noted that the journalist 'did not obtain the information in question by unlawful means and the investigation failed to prove that he had actively sought to obtain such information'.[424] The Court also observed that although journalists have duties and responsibilities, it is for states to 'organise their services and to train their personnel … to ensure that no confidential information is disclosed', ultimately finding that the journalist's conviction constituted a violation of article 10.[425]

Similar reasoning was applied when a court reporter asked an administrative assistant at a prosecutor's office to provide him with confidential documents connected to a high-profile robbery, and was prosecuted for inciting another to disclose official secrets and fined approximately 325 euros.[426] Although it was argued that the court reporter, an 'experienced columnist', should have known the information was confidential, the Court considered it relevant that the reporter had not resorted to trickery or pressure to obtain the information, and that the prosecutor's office played 'an important part of the responsibility for the indiscretion'.[427] The Court ultimately found the reporter's conviction to be disproportionate in light of this conduct.

In contrast, the Court held there was no violation of article 10 when a case file of a controversial murder trial was left in a shopping centre and an unknown person provided a copy to a journalist who was later convicted and fined for publishing the file in a magazine. The Court noted that the fact the journalist had not obtained the material by unlawful means 'is not necessarily a determining factor in assessing whether or not he complied with his duties and responsibilities when publishing the information'.[428] Rather, 'as a professional journalist', he 'could not have been unaware of the confidential nature of the information he was planning to publish'.[429] Considering this alongside the proportionality of the penalty and the impact on the accused's private life and criminal proceedings, the Court held that no violation of article 10 had taken place.

5.2.2. Publication as a last resort?

Another aspect of a whistleblower's conduct that the European Court will closely consider—and that the Tshwane Principles also prioritize—is whether the

[421] Ibid., §77.
[422] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §56.
[423] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018. See s. III.4.2.1. (Type and severity of harm).
[424] Ibid., §§91–92.
[425] Ibid., §92.
[426] ECtHR, *Dammann v. Switzerland* (App. no. 77551/01), 25 April 2006.
[427] Ibid., §55.
[428] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §57.
[429] Ibid., §57.

whistleblower used alternative channels of reporting before publishing secret information. The Court will consider 'whether there was available … any other effective means of remedying the wrongdoing' and have held that 'disclosure should be made in the first place to the person's superior or other competent authority or body' and only where this is 'clearly impracticable … as a last resort, be disclosed to the public'.[430] For example, when the Court found that a journalist's conviction for sharing secret information concerning Romania's military operations in Afghanistan violated his right to free speech, the Court noted that the journalist's first step 'after coming into possession of the information in question was to discuss it with the institution concerned by the leak', and that the institution then made no attempts to recover the documents.[431] And similarly in the *Bucur* case, the Court took into account that there appeared to be no procedure for expressing concerns with Romania's intelligence services other than raising these with superiors, which the employee in question had done.[432] And as the leaks directly concerned superiors, the Court also expressed doubt as to the 'effectiveness of any reports that the applicant may have made'.[433]

Similarly, the Tshwane Principles provide that the law should protect from penalties for disclosures if:

a) the person made the disclosure to an internal or independent oversight body which either refused or failed to investigate, or the person did not receive a reasonable and appropriate outcome within a reasonable and legally defined time period; or
b) the person reasonably believed there was a significant risk that making the disclosure internally or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness or retaliation against the person or a third party; or
c) there were no established bodies to which the disclosure could have been made; or
d) the disclosure related to an act or omission that constituted a serious and imminent risk of danger to the life, health and safety of persons, or to the environment.

The Principles also provide for residual protection even where these conditions have not been met, protecting speakers from retaliation unless the harm of the speech outweighs the public interest in it being disclosed.[434]

5.2.3. 'Responsible journalism'

According to the European Court of Human Rights, the 'protection' afforded to the press as a 'watchdog' in democratic society is 'subject to the proviso that they act in

[430] ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §73.
[431] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §§91–92.
[432] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §§96–98. See s. III.4. (Necessity).
[433] Ibid., §97. See s. III.4. (Necessity). The Court also considered a second route suggested by the government for disclosure, namely the referral to a parliamentary committee, but noted that the MP that was contacted about the leaks was in fact a member of that Committee. Ibid., §§98–99.
[434] Tshwane Principles, Principle 43.

good faith in order to provide accurate and reliable information in accordance with the tenets of responsible journalism'.[435] And although the Inter-American Court has referenced the 'responsible journalism' doctrine, no other international body has used it to determine the outcome of cases involving speech by the press.[436]

The European Court applies the doctrine by addressing three questions. First, it considers whether a journalist has acted unlawfully in the manner in which the information was obtained since journalists are not above the law.[437] The fact that a journalist has breached the law in his or her public interaction with authorities when exercising journalist functions is considered 'a most relevant, albeit not decisive, consideration when determining whether he or she has acted responsibly'.[438] Secondly, 'responsible journalism requires that the journalists check the information provided to the public to a reasonable extent'. In particular, 'special grounds' are required before the media can be dispensed from their 'ordinary obligation to verify' the content they disseminate.[439] And finally, the Court considers the manner of presentation of the speech, recognizing that although a court should not seek to determine 'what technique of reporting should be adopted by journalists', and journalistic freedom allows 'recourse to a degree of exaggeration, or even provocation', this deference is not 'unlimited'.[440]

The Court has applied this doctrine even in circumstances where it does not consider that an impugned publication could be regarded as 'contributing to a debate of public interest' or as constituting 'political speech' so in these cases at least it seems to be establishing a separate standard based on the speaker, and not the subject matter of the

[435] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §84.

[436] See ch. 1 (Introduction), s. II.3.2.5. (Relevance of whether the speaker is a journalist). See IACtHR, *Mémoli v. Argentina* (Series C, no. 265), 22 August 2013, §122 (where 'responsible journalism' is referenced but does not appear to be dispositive of the case).

[437] ECtHR (GC), *Pentikäinen v. Finland* (App. no. 11882/10), 20 October 2015, §90. See also ECtHR, *Brambilla v. Italy* (App. no. 22567/09) 23 June 2016, §64 ("The Court reiterates that the concept of responsible journalism requires that whenever a journalist's conduct flouts the duty to abide by ordinary criminal law, the journalist has to be aware that he or she is liable to face legal sanctions, including of a criminal character'); ECtHR, *Salihu v. Sweden* (App. no. 33628/15), 10 May 2016, §59 (where journalists purchased a firearm to demonstrate the ease of doing so, and the Court held this 'could have been illustrated by other means').

[438] ECtHR (GC), *Pentikäinen v. Finland* (App. no. 11882/10), 20 October 2015, §90. The UK courts in Julian Assange's case also considered the lawfulness of the manner in which the information was acquired as being relevant and potentially dispositive. In the extradition proceedings, experts gave evidence that Assange was 'doing no more than what many investigative reporters in the US already do', as the reporter–source relationship is 'a constant back-and-forth between parties, and good newsgatherers actively solicit their sources for information'. But in finding that these charges were compatible with UK law and article 10 of the European Court, Judge Baraister held that Assange's 'activities went beyond the mere encouragement of a whistle-blower', and that his assistance to Manning in seeking to decipher a code 'most obviously demonstrates' his complicity with her theft and 'separates his activity from that of the ordinary investigative journalist'. She concluded that '[h]ad Mr. Assange decided not to assist Ms. Manning to take the information in [this manner], *and merely received it from her*, then the Article 10 considerations would be different'. See, e.g., UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, Consolidated Annex, 11 January 2021(evidence of Professor Feldstein, §40); UK Westminster Magistrates' Court, *The Government of the United States of America v. Julian Paul Assange*, 11 January 2021, §§96, 99, 118.

[439] ECtHR, *Kącki v. Poland* (App. no. 10947/11), 4 July 2017, §52; ECtHR (GC), *Pedersen and Baadsgaard v. Denmark* (App. no. 49017/99), 17 December 2004, §78; ECtHR, *Flux v. Moldova (No. 6)* (App. no. 22824/04), 29 July 2008, §26.

[440] ECtHR (GC), *Jersild v. Denmark* (App. no. 15890/89), 23 September 1994, §31; ECtHR (GC), *Bladet Tromsø and Stensaas v. Norway* (App. no. 21980/93), 20 May 1999, §§59, 63; ECtHR (GC), *Couderc and Hachette Filipacchi Associés v. France* (App. no. 40454/07), 10 November 2015, §144.

speech.[441] But the doctrine has also been applied to non-journalists, such as human rights activists, NGOs and whistleblowers who engage in public debate and are also considered 'watchdogs'.[442] And the questions that the Court asks—essentially relating to whether the speaker was negligent or reckless as to the falsity of the speech—overlap with the questions the Court deems relevant to any speaker who discloses confidential official data.[443] This means that the responsible journalism doctrine, although in many cases applied in a manner that is protective of journalists, adds unnecessary doctrinal confusion.

5.3. Truth

The truthfulness of a statement will generally be of less significance in the area of official secrets and espionage than, for example, defamatory speech.[444] But truthfulness remains relevant to the analysis of the mental culpability and reasonableness of the conduct of the speaker and is also relevant in assessing whether speech is in the public interest. The European Court has held that the 'authenticity' of information disclosed, and whether it had been 'carefully verified' is one of a number of factors to be balanced when determining the necessity of a restriction to the disclosure of information receiving in confidence.[445] Another 'determinant factor' is the motive behind the actions of the reporting employee, with the Court holding that it is 'important to establish that, in making the disclosure, the individual acted in good faith and in the belief that the information was true'.[446]

The authenticity of leaked information was a key aspect of the leading case of *Bucur*, as the Romanian government argued that the whistleblower in that case had provided false information to the public.[447] The Court 'bore in mind' Resolution 1729 (2010) of the Parliamentary Assembly of the Council of Europe, which provides that any 'whistle-blower shall be considered as having acted in good faith provided he or she had *reasonable grounds to believe* that the information disclosed was true, even if it later turns out that this was not the case, and provided he or she did not pursue any unlawful or unethical objectives'.[448] The Court noted that several factors, uncontested by the Romanian Government, supported the whistleblower's belief that unlawful telephone tapping had taken place but had not been considered by domestic courts.[449] And the judges ultimately held that Mr. Bucur 'had reasonable grounds to believe that the

[441] ECtHR, *Satakunnan Markkinapörssi Oy v. Finland* (App. no. 931/13), 27 June 2017, §§174–178. Cf. Dissenting Opinion of Judges Sajo and Karakas.

[442] ECtHR (GC), *Magyar Helsinki Bizottság v. Hungary* (App. no. 18030/11), 8 November 2016, §159; ECtHR, *Gawlik v. Liechtenstein* (App. no. 23922/19), 16 February 2021, §77.

[443] In addition, the issue of intent or mental fault is relevant to an analysis of all speech under international standards. See ss III.4. (Necessity) and III.5.1. (Public interest defence).

[444] See ch. 2 (Insulting Speech), s. III.4.1. (Truth); HRC, General Comment No. 34 (2011), §47.

[445] ECtHR (GC), *Guja v. Moldova* (App. No. 14277/04), 12 February 2008, §75.

[446] Ibid., §77. As part of its 'responsible journalism' analysis the Court also considers that heightened protection is 'subject to the proviso' that a speaker is 'acting in good faith in order to provide *accurate and reliable* information'. See, e.g., ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §58 (emphasis added). See s. III.5.2.3. ('Responsible journalism').

[447] ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §107.

[448] Ibid., §107 citing Parliamentary Assembly of the COE Resolution 1729(2010) on Protection of 'whistleblowers', 29 April 2010, 6.2.4 (emphasis added).

[449] Ibid., §108.

information disclosed was true', and that he was acting in good faith motivated by respect for Romanian laws and the Constitution.[450]

Certain soft law instruments also incorporate a reasonable belief in the truth of the impugned speech as a condition of, or relevant factor in the assessment of whether penalties are appropriate for leaks of confidential information. The African Commission's 2019 Declaration of Principles on Freedom of Expression provides that all persons should be protected from penalties for disclosures 'in the public interest, in the honest belief that such information is substantially true'.[451] The Tshwane Principles framework protects public officials who have 'reasonable grounds to believe' that information discloses wrongdoing. The Principles also provide that the 'motivation for a protected disclosure [by public officials] is irrelevant except where the disclose is proven to be *knowingly* untrue'.[452]

5.4. Opinion

International standards related to espionage and official secrets laws rarely refer to whether speech disclosing confidential information can be considered an 'opinion', though this is a basis for the exclusion of liability for defamatory speech.[453] The Inter-American Court of Human Rights has however extended the principle that opinion cannot be the object of sanction to the national security context in *Usón Ramîrez v. Venezuela.* In that case, the Court found a violation of free speech rights where Mr. Usón Ramîrez was not stating that a premediated crime had been committed, but that *in his opinion* such a crime seemed to have been committed, and therefore could not be convicted under military slander laws.[454]

6. Penalties

All international human rights bodies consider penalties to be relevant to the assessment of whether a restriction to speech is 'necessary' and can therefore comply with international standards.[455] A number of international human rights bodies have

[450] Ibid., §§107–113, 117–118.

[451] Tshwane Principles, Principle 35.

[452] Tshwane Principles, Principle 38. Although the 'right to truth' concerning human rights violations is an area of jurisprudence beyond the scope of this report, the Tshwane Principles provide that the extent to which a disclosure may 'shed light on the truth' about alleged human rights violations is a relevant factor when determining if information may be disclosed: Principle 10(A)(4). However, the Tshwane Principles' position is that persons who are *not* public personnel should *never* be sanctioned for the dissemination of classified information (Tshwane Principles, Principle 47).

[453] See ch. 2 (Insulting Speech), s. III.4.5. (Opinion).

[454] Cf. IACtHR, *Usón Ramîrez v. Venezuela* (Series C, no. 207), 20 November 2009, §86 (emphasis added). See also IACtHR, *Palamara-Iribarne v. Chile* (Series C, no. 135), 22 November 2005, §§87–88 (finding that, by way of contempt charges, 'Mr. Palamara-Iribarne suffered serious consequences for having voiced his opinion on the manner in which officers of the military justice were conducting the proceedings against him and the manner in which military authorities were treating him and his family').

[455] See, e.g., HRC, General Comment No. 34 (2011), §§34–35; ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §69; IACtHR, *Palamara-Iribarne v. Chile* (Series C, no. 135), 22 November 2005, §85; ACtHPR, *Konaté v Burkina Faso* (App. no. 4/2013), 5 December 2014, §145.

expressed disapproval of criminal sanctions on the basis that it is a disproportionate response to speech, including in the national security context.

The Human Rights Committee has observed that states should exercise 'great caution in the imposition of criminal penalties that punish speech',[456] to the point that a term of imprisonment has *never* been found an appropriate restriction on speech in the Committee's decisions.[457] The Human Rights Committee has also criticized certain spying offences that carry the death penalty under Bangladesh's Official Secrets Act.[458] And the Working Group has asserted that 'a vague and general reference to the interests of national security or public order, without being properly explained and documented, is insufficient to convince the Working Group that … restrictions … by way of deprivation of liberty are necessary'.[459]

The European Court of Human Rights has held that authorities must generally 'show restraint in resorting to criminal proceedings in matters of freedom of expression'.[460] The Court has also warned that a penalty imposed on speech should not 'amount to a form of censorship intended to discourage the press from expressing criticism', particularly when a sanction could deter journalists from 'contributing to public discussion of issues affecting the life of the community'.[461] Consequently, 'the fact of a person's conviction may in some cases be more important than the minor nature of the penalty imposed'.[462]

However, the European Court provides some leeway to states when it comes to criminal penalties for hate speech[463] and has similarly held that 'in cases concerning criminal sanctions for the disclosure of classified military information … the margin of appreciation is to be left to the domestic authorities in matters of national security'.[464]

On this basis, the European Court has in a small number of cases allowed terms of imprisonment for the disclosure of official secrets, particularly where conduct constituted traditional spying offences by public officials, rather than simply speech by journalists or others. For example, where a Russian naval officer allegedly transferred information to Japanese journalists about the Russian navy's military exercises and financial situation, the European Court considered that domestic courts had not 'overstepped the limits of the margin of appreciation … in matters of national security' by convicting the officer of treason, through espionage, and sentencing him to four years' imprisonment.[465] The Court held that the officer had been convicted 'as a serving military officer, and not as a journalist, of treason through espionage for having collected

[456] HRC, *Rabbae v. Netherlands* (Comm. no. 2124/2011), 14 July 2016, Individual Opinion (Concurring) of Committee members Sarah Cleveland and Mauro Politi, §7.
[457] See ch. 1 (Introduction), s. II.3.1.6. (Criminal penalties for speech).
[458] HRC, *Concluding Observations: Bangladesh* (2017) UN Doc. CCPR/C/BGD/CO/1, §§23–24.
[459] WGAD, *Gulmira Imin v. China* (Opinion no. 29/2012), 29 August 2012, §29.
[460] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §81.
[461] Ibid., §79.
[462] Ibid., §79.
[463] See ch. 1 (Introduction), s. III.3.1.1. (Justification for penalizing speech).
[464] ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §96, citing ECtHR, *Hadjianastassiou v. Greece* (App. no. 12945/87), 16 December 1992, §47.
[465] ECtHR, *Pasko v. Russia* (App. no. 69519/01), 22 October 2009.

and kept, with the intention of transferring it to a foreign national, information of a military nature that was classified as a State secret', and considered the sentence to be 'very lenient'.[466]

And where an air force engineer was sentenced by a Greek military court to a suspended sentence of five months' imprisonment for disclosing his technical knowledge about a missile for commercial gain, the Court considered it necessary to account for the 'specific "duties" and "responsibilities" incumbent on the members of the armed forces' and held that the Greek courts had not overstepped the 'margin of appreciation' left to domestic authorities on national security matters.[467]

But the European Court has also been clear that the discretion left to states in such cases is not unlimited. As a result, the Court found a violation of article 10 where a journalist had been ordered to pay a fine of 870 Euros after sharing 'secret' information concerning Romanian military operations with colleagues.[468] While noting that a margin of appreciation applies to penalties in matters of national security, the Court held that 'the applicant in the current case is a journalist claiming to have made the disclosure in the context of a journalistic investigation and not a member of the military who collected and transmitted secret military information to foreign nationals' and that the penalty was, accordingly, 'not reasonably proportionate to the legitimate aim pursued'.[469]

The Inter-American Court of Human Rights has also voiced a strong rebuke to criminal sanctions even in a national security context in *Palamara-Iribarne v. Chile*.[470] In that case, Mr. Palamara-Iribane, a naval mechanic engineer, was sentenced to a 61-day prison term, a fine and suspension from public office for contempt, after he criticized the way military authorities responded to him publishing a book regarding ethical standards within military intelligence. The Court noted that criminal law is 'the most restrictive and severe means of imposing liability for illegal conduct', and that Mr. Palarmara-Iribarne had suffered 'serious consequences', including four days in pre-trial custody. And it ultimately held that the 'sanctions were disproportionate to the criticism levelled at government institutions and their members, thus suppressing debate, which is essential to the functioning of a truly democratic system, and unnecessarily restricting the right to freedom of thought and expression'.[471]

Similarly, the African Court on Human and Peoples' Rights has held that custodial sentences for violations of the laws of freedom of speech are generally inappropriate, and will only be lawful in 'serious and very exceptional circumstances' such as 'incitement to international crimes, public incitement to hatred, discrimination or violence

[466] Ibid., §§86–87.
[467] ECtHR, *Hadjianastassiou v. Greece* (App. no. 12945/87), 16 December 1992, §44–47.
[468] This amount was a combination of a fine and judicial costs. ECtHR, *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §§96–99.
[469] Ibid.
[470] IACtHR, *Palamara-Iribarne v. Chile* (Series C, No. 135), 22 November 2005. See s. III.1. (International standards related to speech affecting national security).
[471] Ibid., §88.

or threats against a person or group of people, because of specific criteria such as race, colour, religion and nationality'.[472]

The Tshwane Principles provide that, even if public personnel are not protected by the public interest framework the Principles advocate, they should not be subjected to criminal penalties.[473] If criminal penalties are used, they should only apply to 'narrow categories of information that are clearly set forth in law'.[474] Penalties for disclosures which 'pose a real and identifiable risk of causing significant harm' should be 'proportional to the harm caused' and the catch-all public interest defence provided by the Principles must be available.[475] And according to the 2013 Joint Declaration by the UN and OAS Special Rapporteurs on freedom of expression, the imposition of criminal sanctions for the disclosure of confidential information 'must be exceptional and strictly limited according to necessity and proportionality'.[476]

IV. Recommendations

The following recommendations are based on minimum international human rights standards applicable to espionage and official secrets laws. Where there is a divergence or lacuna in such standards, we advocate for a best practice based on national systems or emerging international standards. A common theme articulated in these recommendations is the significant disconnect between international minimum standards and state laws on espionage and official secrets. Despite increasingly crystallized international standards which, at a minimum, necessitate clear harm thresholds and consideration of the public interest in disclosure, many state laws fall short, even in leading democracies.

A further theme of these recommendations is the primacy given to the Tshwane Principles. Drafted by 17 organizations and five academic centres, in consultation with 500 experts across the globe, including government officials and military officers, and endorsed by UN and regional Special Rapporteurs in the space, we consider these Principles to be highly persuasive.[477] The Principles' requirement that states recognize a public interest defence is a particularly compelling extension of existing international standards that we endorse. But it cannot provide sufficient protection for speech in the

[472] ACtHPR, *Konaté v Burkina Faso* (App. no. 4/2013), 5 December 2014, §165. Although this case grapples with criminal defamation laws, it reflects the Court's reluctance to consider criminal penalties for expression proportionate in any circumstances. Cf. *Federation of African Journalists v. Gambia,* where the Community Court of Justice of ECOWAS held that the practice of imposing criminal sanctions for sedition, defamation and false news publication has a chilling effect that may unduly restrict journalists' freedom of expression: ECOWAS CCJ, *Federation of African Journalists v. Gambia* (Suit no. ECW/CCJ/APP/36/15), 13 February 2018.

[473] Tshwane Principles, Principle 46.

[474] Tshwane Principles, Principle 46(b).

[475] Tshwane Principles, Principle 46(b). See s. III.5.1. (Public interest defence).

[476] UN Special Rapporteur & OAS Special Rapporteur, Joint declaration on surveillance programs and their Impact on freedom of expression (2013) ('Any attempt to impose subsequent punishment on those who reveal classified information must be based on previously established laws applied by impartial and independent bodies with full due process guarantees, including the right to appeal the ruling'). See also, e.g., Johannesburg Principles, Principle 22.

[477] Open Society Justice Initiative, 'Understanding the Tshwane Principles' (12 June 2013).

absence of laws that are holistically fair: for instance, by also requiring proof of harm and proportionate penalties. The recommendations below should therefore be considered in their entirety.

1. Espionage and official secrets laws must not be vague or overbroad.

Espionage and official secrets laws must be 'accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction'.[478] Laws must be 'formulated with sufficient precision to enable the person concerned to regulate his or her conduct'.[479] Anachronistic terms whose meaning is unclear in the modern day, such as 'enemy'—which is used in dozens of colonial-era laws that are still on the books—and 'subversion', are unlikely to satisfy this legality requirement.[480] Neither will laws that effectively leave what constitutes an offence 'to the discretion of the authorities', like Cambodia's use of the phrasing 'undermin[ing] the national defence'.[481]

2. States must provide adequate reasons to justify penalties for speech on the grounds of 'national security'. Classification of information as 'secret' is not in itself a sufficient basis for penalizing the disclosure of information. Protecting the reputation of governments, government organs or state officials is not a legitimate 'national security' interest that can serve as a basis to penalize speech.

States should clearly define national security in their espionage and official secrets laws.[482] The fact that information has been 'classified' does not in itself demonstrate that secrecy is justified.[483] Information in the public domain, even in circumstances

[478] Tshwane Principles, Principle 3(a). See also Johannesburg Principles, Principle 1.1(a).
[479] ECtHR (GC), *Perinçek v. Switzerland* (App. no. 27510/08), 15 October 2015, §131.
[480] See UK Law Commission, *Protection of Official Data Report* (2020), §§3.88–3.110. See also UK Law Commission, *Protection of Official Data: A Consultation Paper* (2017), §2.164.
[481] WGAD, *Chhin v. Cambodia* (Opinion no. 3/2019), 24 April 2019, §49. Some laws misuse presumptions to impose guilt in an overbroad manner. Because this concerns general criminal law principles this issue is beyond the scope of the book, but relevant guidance can be found in A. Clooney & P. Webb, *The Right to a Fair Trial in International Law* (OUP 2021), ch. 4. See s. II.2.2.3. (Cambodia).
[482] Tshwane Principles, definition of 'legitimate national security interest'. This recommendation is intended to cover not only criminal sanctions but also potentially civil penalties, even though the review of state practice has shown that these laws are usually criminal in nature. Other recommendations, in particular Recommendations 3–5, all explicitly relate only to criminal laws.
[483] WGAD, *Lee Kun-hee v. South Korea* (Opinion no. 29/1994), 29 September 1994, §6. See also ECtHR (C), *Vereniging Weekblad Bluf! v. Netherlands* (App. no. 16616/90), 9 February 1995, §41, ECtHR, *Görmüş v. Turkey* (App. no. 49085/07), 19 January 2016, §62.

where it was previously afforded a high degree of protection, is not 'sufficiently sensitive' to warrant restrictions under official secrets laws.[484] And states must interpret the concept of national security 'with restraint'.[485] They must also allow domestic courts to have access to sufficient information to effectively assess whether national security interests are at stake.[486]

A restriction on speech on national security grounds is not legitimate 'unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government'.[487] States cannot restrict speech on the basis of the 'general situation in the country: they must demonstrate a 'specific and individualized' threat to national security.[488] And definitions of national security such as Australia's, which encompass 'the country's political, military or economic relations with another country or other countries' are overbroad.[489]

If states adopt a list of categories of information that must be kept secret to protect a legitimate national security interest, these should be narrowly defined.[490] States may also incorporate a list of information which is not—or is presumed not to be—secret.[491]

Protecting the reputation of governments, government organs or state officials is not a legitimate 'national security' interest that can serve as a basis to penalize speech. International bodies have also made clear that the following do *not* constitute national security interests:

- Protecting a government or its officials from embarrassment or exposure of wrongdoing;
- Preventing disclosure of information about the functioning of public institutions;
- Preventing disclosure of information about human rights violations or other serious violations of law;[492]
- Preventing disclosure of evidence pertaining to 'environmental conditions, emergencies and disasters posing a risk to human life and health';[493]

[484] See, e.g., ECtHR (C), *Vereniging Weekblad Bluf! v. Netherlands* (App. no. 16616/90), 9 February 1995, §§41–46; ECtHR, *Observer and Guardian v. United Kingdom* (App. no. 13585/88), 26 November 1991, §§69–70; Tshwane Principles, Principle 49(b); Johannesburg Principles, Principle 17; IACtHR, *Palamara-Iribarne v. Chile* (Series C, no. 135), 22 November 2005, §77; Parliamentary Assembly of the COE, Resolution 1551 on Fair trial issues in criminal cases concerning espionage or divulging state secrets, 19 April 2007, §10.1. Some dated or historical information may also fall into this category. See, e.g., WGAD, *Xiyue Wang v. Iran* (Opinion no. 52/2018), 23 August 2018, §§32–33; ECtHR (Plenary Court), *The Observer and The Guardian v. United Kingdom* (App. no. 13585/88), 26 November 1991, §§69–70; ECtHR (C), *Vereniging Weekblad Bluf! v. Netherlands* (App. no. 16616/90), 9 February 1995, §§41–46.

[485] See ECtHR, Guide on Article 10 of the Convention, 31 August 2022, §543, citing ECtHR (GC), *Stoll v. Switzerland* (App. no. 69698/01), 10 December 2007, §54.

[486] ECtHR (GC), *Janowiec v. Russia* (App. nos 55508/07 & 29520/09), 21 October 2013, §213.

[487] Johannesburg Principles, Principle 2(a).

[488] HRC, General Comment No. 34 (2011), §35.

[489] See Australian Criminal Code Act s. 90.4(1).

[490] See, e.g., Tshwane Principles, Principle 9. See s. III.4.1. (Secrecy). These categories are provided by the Tshwane Principles as 'information that legitimately may be withheld'.

[491] Tshwane Principles, Principle 10. See s. III.4.1. (Secrecy).

[492] Tshwane Principles, Principle 10; WGAD, *Li Hai v. China* (Opinion No. 19/1999) 16 September 1999, §12.

[493] Tshwane Principles, Principle 10; WGAD, *Grigorii Pasko v. Russian Federation* (Opinion No. 9/1999), 20 May 1999, §7.

- Entrenching or strengthening a particular ideology, political interest or party;
- Suppressing industrial unrest;
- Suppressing lawful protests.[494]

3. Criminal liability under official secrets and espionage laws should be conditional on the demonstration of a sufficiently high mental culpability by the speaker, a showing of an objective probability of serious harm caused by the speech and be subject to a 'public interest' defence.

3.1. *Mens rea requirement:* Criminal liability under official secrets and espionage laws should be conditional on the demonstration of a sufficiently high mental culpability by the speaker.

Speech should only be prosecuted under espionage or official secrets laws if a prosecutor can prove that the speaker intended to disclose the secret material and intended to harm national security interests.[495] States should expressly provide for a high *mens rea* standard in official secrets laws, particularly those of a criminal nature, to justify restricting speech and any criminal penalties.[496] This intent requirement should be accompanied by a high harm and causation threshold, rather than be a replacement for such requirements, as has been suggested by the Law Commission.[497]

Although international human rights bodies have rarely opined on the precise intent requirements for official secrets and espionage laws, international standards are clear that the intent of a speaker is a relevant factor in determining the necessity of any restriction of the right to free expression under international law. International bodies have found that to ensure compliance with the principle of legality, states should explicitly provide a precise and sufficiently high intent element within their secrecy and espionage laws.[498] And the European Court makes clear that a determining 'factor in deciding whether a particular disclosure should be protected or not' is the motive of the whistleblower, considering it 'important to establish that, in making the disclosure, the individual acted in good faith and in the belief that the information was true that it was in the public interest to disclose it and that no other, more discreet, means of remedying the wrongdoing was available to him or her'.[499] In addition, the Tshwane Principles

[494] Johannesburg Principles, Principle 2(b); Tshwane Principles, definition of 'legitimate national security interest'.

[495] In some legal systems this may include recklessness as to such harm being created. See ch. 3 (Hate Speech), s. VI.3.1 (Recommendations) and ch. 4 (False Speech), s. IV.6 (Recommendations).

[496] This can include an assessment of whether publication was a last resort, whether the person disclosing the information tried to report the issue being disclosed internally before publishing, and so on.

[497] See s. II.2.1.1. (United Kingdom). See UK Law Commission, *Protection of Official Data Report* (2020) §4.15.

[498] See, e.g., IACtHR, *Usón Ramírez v. Venezuela* (Series C, no. 207), 20 November 2009, §56; ECOWAS CCJ, *Federation of African Journalists v. Gambia* (Suit No. ECW/CCJ/APP/36/15), 13 February 2018.

[499] ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §77. See s. III.5.1. (Public interest defence), s. III.5.2. (Reasonableness of the publication), s. III.5.3. (Truth).

also provide that a public interest defence should be available to those who 'reasonably believed' both that they were disclosing wrongdoing and that the public interest in the information being revealed outweighed any harm that would be caused by its publication.[500]

The 'intent' formulation put forward by the Law Commission presents some challenges. The Commission has suggested the following test: 'that the defendant (i) knew; (ii) believed; or (iii) was reckless as to whether the disclosure (a) would cause damage; (b) was likely to cause damage; (c) risked causing damage; or (d) was *capable of* causing damage'.[501] Media organizations have criticized this test, arguing that 'if you have been told by an official that a disclosure would be damaging, but have good reason not to believe it, you might still commit an offence—because having been told you may now have reasonable cause to believe that it is "capable" of being so'.[502] The BBC stated that 'the use of the words "capable of" would significantly lower the threshold of criminal liability as it could encompass disclosure which has only a remote possibility of causing damage'.[503] And the Guardian News and Media complained that this 'means that a disclosure which is *unlikely* to cause damage may nevertheless be an offence because in circumstances that are highly unlikely to ever arise, it *might* cause damage'.[504] They point out that in practice, editors ask 'is this information damaging or is it embarrassing', and that the proposed amendment is 'a much less certain and much more subjective test'.[505] We agree with these concerns and urge states to adopt clear and sufficiently rigorous intent requirements.

3.2. Harm requirement: States should only criminalize speech when they can prove that there was an objective probability that the speech would cause serious harm such as violence, a serious criminal offence or endangerment to human life.

International standards make clear that espionage and official secrets laws must establish a 'direct and immediate connection between the expression and the threat' of

[500] Tshwane Principles, Principles 38, 40. The Principles also note that it is 'ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection': Principle 40. The Principles distinguish intent from motive, noting that the motive for disclosing information should be irrelevant 'except where the disclosure is proven to be knowingly untrue': Principle 38.

[501] UK Law Commission, *Protection of Official Data Report* (2020), Recommendation 11 (emphasis supplied). The ECtHR has previously applied a similar test of whether speech would be 'capable of' causing harm in relation to hateful and terror-related speech: see ch. 3 (Hate Speech), s. III.2.3.1 (Harm). See also ch. 6 (Speech related to National Security: Terrorism Laws), s. III.3.1 (Harm).

[502] Guardian News & Media, *Response to Law Commission Consultation Paper no 230 on protection of Official Data* (2017), 55.

[503] UK Law Commission, *Protection of Official Data Report* (2020), §4.67. The UK Law Commission recognized 'the weight of consultees' strong opposition to this recommendation', but considered these concerns would be addressed by 'fortifying and balancing this recommendation with the public interest disclosure recommendations': §4.80. The British Government strongly agreed with the UK Law Commission's proposal to create an explicit fault element 'on the assumption that the fault element will remain as construed in *Keogh*', as any higher test 'would compound the difficulties of prosecuting the offence': §4.71.

[504] Guardian News & Media, *Response to Law Commission Consultation Paper no 230 on protection of Official Data* (2017), 55; UK Law Commission, *Protection of Official Data Report* (2020), Recommendation §4.55.

[505] Guardian News & Media, *Response to Law Commission Consultation Paper no 230 on protection of Official Data* (2017), 53-4.

harm[506] and states must demonstrate a link between the speech they seek to penalize and 'in specific and individualized fashion the precise nature of the threat' that may result from such speech.[507] International bodies have also made clear that the harm must be serious. For example, the European Court has found a violation of article 10 when a state has argued that the harm justifying official secrets laws is 'the interest in maintaining public confidence in [an] institution'.[508] The Tshwane Principles provide that harm must be 'significant' and the Johannesburg Principles suggest that speech can only be sanctioned on the grounds of national security if this is likely to 'incite imminent violence'.[509]

We recommend that speech only be restricted when there is an objective probability (meaning that it is more probable than not) of serious harm that is direct and imminent. This standard should be set out in national laws.[510] This high bar is preferable to lower standards such as in the United States, where criminal penalties may apply to the disclosure of information that 'would be *potentially damaging* to the United States or *might be* useful' to an enemy, or the UK standard of 'likelihood' of damage.[511] We also recommend that states limit the use of espionage and official secrets laws to harm that takes the form of violent or illegal acts[512] that may cause serious physical injury or death through speech. These causation and harm requirements should exist alongside high intent standards.[513]

This recommendation is at odds with the Law Commission of England and Wales proposal to remove the requirement to prove 'damage' or the likelihood of damage for unauthorized disclosure for offences committed by public servants in national law. The Law Commission and UK Government suggest that a whistleblower's culpability is the same whether or not the disclosure has been damaging.[514] And they argue that proving harm is too difficult: it 'can make it difficult to bring a prosecution'.[515] The UK Government has suggested that this is because of the requirement to place highly

[506] See s. III.4.2. (Harm); HRC, General Comment No. 34 (2011), §35. Cf. the ACmHPR, Declaration of Principles of Freedom of Expression and Access to Information (2019) (requiring 'a close causal link between the risk of harm and the expression').

[507] HRC, General Comment No. 34 (2011), §35. See also UN Special Rapporteur D. Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Disease pandemics and the freedom of opinion and expression* (2020) UN Doc. A/HRC/44/49, §15.

[508] See s. III.4.2.1. (Type and severity of harm); ECtHR, *Bucur and Toma v. Romania* (App. no. 40238/02), 8 January 2013, §115; ECtHR, *Görmüş v. Turkey* (App. no. 49085/07), 19 January 2016, §63.

[509] Johannesburg Principles, Principle 6.

[510] See IACtHR, *Usón Ramirez v. Venezuela* (Series C, no. 207), 20 November 2009, §56 (where the Inter-American Court criticized a military slander provision on the basis that the article did 'not specify the injury required', and therefore 'such law allows that the subjectivity of the offended party determine the existence of the crime').

[511] See s. III.4.2. (Harm); Feuer (n 7) 117, citing D. McCraw & S. Gikow, 'The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World' (2013) 48 *Harvard Civil Rights-Civil Liberties Law Review* 473, 492 (emphasis added); UK Official Secrets Act 1989 ss 1–6 (see, e.g., ss 1(4)(b), 3(2)(b)).

[512] Assuming these do not themselves violate international human rights law due to overbreadth or on other grounds.

[513] See s. IV.3.1. (Recommendations).

[514] See s. II.2.1.1. (United Kingdom).

[515] UK Law Commission, *Protection of Official Data Report* (2020), §§4.12–4.18.

sensitive information before juries so as to prove damage[516] and that, as a result, prosecutions under the Official Secrets Acts are 'challenging and rare'.[517]

The Law Commission also overstate the problem. In the United Kingdom—and across the world—domestic courts implement a range of safeguards to ensure that evidence on national security proceedings can be adduced. As argued by the Guardian News and Media, 'day in day out, FOI tribunals are dealing with the question of whether disclosures are 'likely' to harm defence, international relations, law enforcement—without causing the enormous harm [the Law Commission] see as inevitable'.[518] In addition, other elements—such as proving a fault element and assessing a 'public interest' defence[519]—'would *still* require the prosecution to show that a disclosure would cause damage', and would '*still* require an explanation of how that damage would be caused'.[520] Citing prosecutions such as that against journalist Duncan Campbell, 'simply for reporting the *existence*' of the United Kingdom's signals intelligence service, civil rights organization Liberty argued that 'the lesson of many of the trials under the Official Secrets Act is not that they have harmed national security, but that they have simply been embarrassing to Government'.[521] Prosecutions may also be rare under official secrets laws because of the infrequency with which these crimes are committed, rather than challenges with the laws themselves.

And such proposals to remove proof of harm requirements run contrary to international standards and provide insufficient safeguards to speech.[522] The damage caused by speech is one of the five factors articulated by the European Court of Human Rights in *Guja v. Moldova* as central to the question of proportionality.[523] Ignoring this central tenet of proportionality is particularly troubling given that the Law Commission has recommended a seven-fold increase in criminal penalties for such speech.

[516] Ibid., §4.14.

[517] UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (May 2021), 14, 18.

[518] Guardian News & Media, *Response to Law Commission Consultation Paper no 230 on protection of Official Data* (2017), 5. See also Campaign for Freedom of Information and Article 19, 'Joint Response to Law Commission Consultation Paper' (4 May 2017), §§16–17. See further UK Law Commission, Protection of Official Data: A Consultation Paper (2017), §3.143, citing G. Robertson, 'Freedom, the Individual and the Law' (Law Commission, 1993), 167, where the Law Commission noted 'our research stands in contrast to those commentators who expressed the view that the damage requirement would be easy to satisfy'.

[519] The Commission suggests that an explicit fault (*mens rea*) requirement and the introduction of a public interest defence will act as sufficient safeguards against the removal of the requirement to prove damage. See UK Law Commission, *Protection of Official Data Report* (2020), §4.15. See s. II.2.1.1. (United Kingdom). But it concedes that '[d]amage and the public interest are not necessarily mutually exclusive concepts', with a public interest defence allowing a defendant to argue that the disclosure was in the public interest *despite* the fact it was damaging'. UK Law Commission, *Protection of Official Data Report* (2020), §4.45.

[520] Campaign for Freedom of Information and Article 19, 'Joint Response to Law Commission Consultation Paper' (4 May 2017), §18.

[521] Liberty Human Rights Organization, 'Liberty's Response to the Law Commission's Consultation on Official Secrecy' (May 2017), §11.

[522] See s. II.2.1.1. (United Kingdom).

[523] See s. III.5.1. (Public interest defence).

3.3. Prosecutions under espionage and official secrets laws should be subject to a 'public interest' defence.

At a minimum, under current international standards, states must balance the public interest in the disclosure of information implicating national security with the harm a disclosure may cause.[524] Laws like the US Espionage Act that do not allow a judge to consider the public interest in their assessment of whether criminal liability is appropriate for speech are not compatible with international minimums standards. States must ensure when applying espionage and official secrets laws that the public interest in the speech is considered in any assessment of the necessity and proportionality of criminalizing it.

In our view, public interest should be an affirmative defence to criminal liability, as set out in the Tshwane Principles.[525] Under these Principles, the speaker must have actually held the belief that the public interest in having the information revealed outweighed the harm in its disclosure, and it must have been reasonable for them to hold that belief. The objective arm of this test ensures that individuals will be held to an appropriately high standard. The Principles also take into account the fact that a disclosure should include only the amount of information 'reasonably necessary to bring to light the wrongdoing'. By balancing between harm and public interest, this public interest defence does not create a *carte blanche* rule where speech involving a matter of public interest is always lawful. Disclosures which intentionally and foreseeably cause very serious harm are likely to outweigh the public interest in disseminating such information and will continue to be sanctioned under official secrets laws, although public interest factors could still in such a case be relevant to mitigation.

This public interest formulation should be preferred to other more narrowly tailored defences which do not sufficiently protect speech. An example is the Australian public interest defence, which is restricted to those engaged in the business of reporting news.[526] This defence arguably leaves vulnerable non-traditional actors in the media space, such as bloggers, as well as sources and human rights groups. Similarly, Canada's public interest defence is unduly narrow as it is only available to individuals 'bound by secrecy', meaning it assists civil servants but provides no protection for journalists.[527]

On the other hand, the suggestion by the Law Commission that a public interest defence should be inserted into the UK Official Secrets Act 1989 is an encouraging development which we fully support. We disagree with the UK Government that the existing UK Official Secrets Act, which pays no regard to the public interest, is compatible with European Court jurisprudence.[528] At a minimum, the European Court considers

[524] See s. III.5.1. (Public interest defence); see, e.g., HRC, General Comment No. 34 (2011), §30. See also Tshwane Principles, Principle 38.
[525] Tshwane Principles, Principle 43.
[526] Australian Criminal Code Act s. 122.5(6).
[527] See s. II.1.4.1. (Public interest).
[528] UK Home Office, *Legislation to Counter State Threats (Hostile State Activity) Government Consultation* (May 2021), 24, 64.

the public interest a relevant criterion in determining the necessity and proportionality of restricting speech.[529] We consider that the defendant's reasonable belief that disclosure was in the public interest is the appropriate test for this defence, consistently with the Tshwane Principles. This formulation provides an appropriate balance by incorporating both subjective and objective considerations.[530]

4. Decisions on arrests and criminal charges under official secrets laws should be approved by a senior authority such as the Minister of Justice, Attorney-General, police chief or chief prosecutor and/or independent expert.

Although international standards do not expressly require this, mandating an extra layer of consent from an official or at higher levels of police and prosecutorial authorities can be an important safeguard against abuse of espionage laws that can produce chilling effects even if any charges are eventually dismissed.[531] This proposal is consistent with Australian, American, Canadian, Ghanaian and Singaporean laws or policies.[532] Alternatively, and ideally, states should adopt a policy whereby an independent expert's consent is required.[533]

5. Criminal sanctions for espionage and official secrets laws should only be used in exceptional circumstances.

The proportionality of penalties imposed on speech is a key element of international standards regulating freedom of speech.[534] The imposition of criminal sanctions, especially imprisonment, for the disclosure of confidential information must be exceptional, and should only apply to disclosures of narrow categories of information set forth in law, that would objectively probably cause serious damage, were committed with a high intent element and are not in the public interest.[535] And governments

[529] ECtHR (GC), *Bédat v. Switzerland* (App. no. 56925/08), 29 March 2016, §49. See, similarly, ECtHR (GC), *Sürek v. Turkey* (*No. 2) (*App. no. 24122/94), 8 July 1999, §34, citing *Wingrove v. United Kingdom* (App. No. 17419/90), 25 November 1996, §58.

[530] Cf. UK Law Commission, *Protection of Official Data Report* (2020). The UK Law Commission did not detail 'the factors that courts and juries must take into account when deciding whether the defence is made out', noting that it did not have the 'evidence necessary to draft with confidence on these matters': §11.8. However, the UK Law Commission concluded that 'it does not serve the public interest to excuse those who damage national security simply because they believed that the disclosure was in the public interest': §11.78.

[531] Reporters Without Borders (RSF) considers express consent must be given by an independent judicial authority, i.e., a court or an investigating judge in civil law countries.

[532] See s. II.1. (Overview of Laws Regulating Disclosure of 'Secret' Material).

[533] See ch. 4 (False Speech), s. IV.7. (Recommendations).

[534] See, e.g., HRC, General Comment No. 34, §§34–35; ECtHR, *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §78.

[535] See ss IV.1. and IV.3. (Recommendations).

should distinguish between state officials who have assumed a 'duty of confidence' and members of the public not bound by such a duty when determining appropriate penalties,[536] as states such as Norway, Bolivia and Belgium have already adopted this practice.[537]

[536] See, e.g., ECtHR (GC), *Guja v. Moldova* (App. no. 14277/04), 12 February 2008, §§70–73; ECtHR (C), *Gîrleanu v. Romania* (App. no. 50376/09), 26 June 2018, §§86, 90–93. A number of soft law instruments, including the Tshwane Principles and the OAS Joint Declaration on Access to Information and on Secrecy Legislation, go further and state that only state officials should be subject to such laws. See, e.g., Tshwane Principles, Principle 47; OAS, Joint Declaration on Access to Information and on Secrecy Legislation, 6 December 2004 ('Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately secret information under their control. Other individuals, including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information'). This requirement is 'not [however] intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information'. Tshwane Principles, Principle 47.

[537] See, e.g., Belgium Criminal Code Arts 118–120, Bolivia Decree Law 10426 Arts 111, 115; Bolivian Military Criminal Code 2002, Arts 56, 58; German Criminal Code ss 94–96, 353b; Norwegian Criminal Code s. 124(a) and (b).

Human Rights Institute